Elementary Abelian Subgroups in p-Groups of Class 2

THÈSE N^{O} 4458 (2009)

PRÉSENTÉE LE 23 JUILLET 2009

À LA FACULTÉ SCIENCES DE BASE

INSTITUT DE GEOMETRIE, ALGEBRE ET TOPOLOGIE

CHAIRE DE THEORIE DES GROUPES

PROGRAMME DOCTORAL EN MATHÉMATIQUES

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

POUR L'OBTENTION DU GRADE DE DOCTEUR ÈS SCIENCES

PAR

David BORNAND

acceptée sur proposition du jury:

Prof. M. Troyanov, président du jury
Prof. J. Thévenaz, directeur de thèse
Prof. S. Bouc, rapporteur
Prof. K. Hess Bellwald, rapporteur
Dr R. Stancu, rapporteur

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Suisse
2009

Résumé

Tous les résultats de ce travail concernent les p-groupes finis, où p est un nombre premier arbitraire. Le premier chapitre traite de classifications de certaines classes de p-groupes de classe 2. Il n'y a pas de résultats significativement nouveau dans ce chapitre, qui sert essentiellement d'introduction à la suite du travail. Cependant, l'approche "géométrique" que nous présentons diffère de l'approche standard, et cela plus particulièrement dans le cas des p-groupes de classe 2 avec centre cyclique. Cette "géométrie" se révèle toutefois particulièrement utile pour la description des groupes d'automorphismes, qui fait l'objet du Chapitre 3.

Les résultats obtenus au Chapitre 2 sont de nature géométrique, puisqu'ils concernent l'étude des intervalles supérieurs dans l'ensemble ordonné $\mathcal{A}_p(P)$, lorsque P est un p-groupe. Grâce aux travaux de Bouc et Thévenaz [8], nous savons déjà que l'ensemble ordonné $\mathcal{A}_p(P)_{\geq 2}$ a le type d'homotopie d'un bouquet de sphères. A la Section 2.4, nous obtenons une borne supérieure, dépendant uniquement de l'ordre du groupe, pour la dimension des sphères présentes dans le type d'homotopie de l'ensemble ordonné $\mathcal{A}_p(P)_{\geq 2}$. Plus précisément, nous montrons que si P est un p-groupe d'ordre p^n, alors $\tilde{H}_k(\mathcal{A}_p(P)_{\geq 2}) = 0$ lorsque $k \geq \lfloor \frac{n-1}{2} \rfloor$. Dans cette même section, nous donnons de plus une caractérisation des p-groupes pour lesquels cette borne est atteinte.

Les résultats principaux de la Section 2.3 sont des valeurs numériques pour le nombre de sphères apparaissant dans le type d'homotopie de l'ensemble ordonné $\mathcal{A}_p(P)_{\geq 2}$ et leur dimension, lorsque P est un p-groupe dont le sous-groupe dérivé est cyclique.

En nous appuyant sur les résultats de la Section 2.3, nous déterminons à la Section 2.5 pour lesquels des p-groupes avec sous-groupe dérivé cyclique l'ensemble ordonné $\mathcal{A}_p(P)$ est homotopiquement Cohen-Macaulay.

La Section 2.7 est une tentative de généralisation des travaux de Bouc et Thévenaz [8] concernant le type d'homotopie de l'ensemble ordonné $\mathcal{A}_p(P)_{\geq 2}$. Comme résultat principal de cette section, nous montrons l'existence d'une suite spectrale E^1_{rs} convergeant vers $\tilde{H}_{r+s}(\mathcal{A}_p(P)_{>Z})$, pour n'importe quel sous-groupe $Z \in \mathcal{A}_p(P)$. En guise d'exemple, nous montrons par ailleurs comment cette suite spectrale peut être utilisée pour retrouver les résultats de Bouc et Thévenaz.

A la Section 2.8, nous donnons des contre-exemples à certains résultats de Fumagalli [12]. Comme principale conséquence, la question de savoir si l'ensemble ordonné $\mathcal{A}_p(G)$ a le type d'homotopie d'un bouquet de sphères lorsque G est résoluble, semble rester une question ouverte.

Les résultats obtenus au Chapitre 3 sont de nature plus algébrique et concernent les groupes d'automorphismes de p-groupes. Le résultat principal de ce chapitre est une description de $\mathrm{Aut}(P)$, lorsque P est un p-groupe d'un des deux types suivants:

(I) p-groupes avec un sous-groupe de Frattini cyclique ($p \geq 2$).

(II) p-groupes de classe 2 avec centre cyclique et dont le quotient par le centre est homocyclique (p impair).

Mots clés: Groupes finis, Ensembles ordonnés, Posets, Complexes de sous-groupes, Intervalles supérieurs, Automorphismes.

Abstract

All the results in this work concern (finite) p-groups. Chapter 1 is concerned with classifications of some classes of p-groups of class 2 and there are no particularly new results in this chapter, which serves more as an introductory chapter. The "geometric" method we use for these classifications differs however from the standard approach, especially for p-groups of class 2 with cyclic center, and can be of some interest in this situation. This "geometry" will for instance, prove to be particularly useful for the description of the automorphism groups performed in Chapter 3. Our main results can be found in chapters 2 and Chapter 3.

The results of Chapter 2 have a geometric flavour and concern the study of upper intervals in the poset $\mathcal{A}_p(P)$ for p-groups P. We already know from work of Bouc and Thévenaz [8], that $\mathcal{A}_p(P)_{\geq 2}$ is always homotopy equivalent to a wedge of spheres. The first main result in Section 2.4, is a sharp upper bound, depending only on the order of the group, to the dimension of the spheres occurring in $\mathcal{A}_p(P)_{\geq 2}$. More precisely, we show that if P has order p^n, then $\tilde{H}_k(\mathcal{A}_p(P)_{\geq 2}) = 0$ if $k \geq \lfloor \frac{n-1}{2} \rfloor$. The second main result in this section is a characterization of the p-groups for which this bound is reached.

The main results in Section 2.3 are numerical values for the number of the spheres occurring in $\mathcal{A}_p(P)_{\geq 2}$ and their dimension, when P is a p-group with a cyclic derived subgroup. Using these calculations, we determine precisely in Section 2.5, for which p-groups with a cyclic center, the poset $\mathcal{A}_p(P)$ is homotopically Cohen-Macaulay.

Section 2.7 is an attempt to generalize the work of Bouc and Thévenaz [8]. The main result of this section is a spectral sequence E^1_{rs} converging to $\tilde{H}_{r+s}(\mathcal{A}_p(P)_{>Z})$, for any $Z \in \mathcal{A}_p(P)$. We show also that this spectral sequence can be used to recover Bouc and Thévenaz's results [8].

In Section 2.8, we give counterexamples to results of Fumagalli [12]. As an important consequence, Fumagalli's claim that $\mathcal{A}_p(G)$ is homotopy equivalent to a wedge of spheres, for solvable groups G, seems to remain an open question.

The results of Chapter 3 are more algebraic and concern automorphism groups of p-groups. The main result is a description of $\mathrm{Aut}(P)$, when P is any group in one of the following two classes:

(I) p-groups with a cyclic Frattini subgroup.

(II) odd order p-groups of class 2 such that the quotient by the center is homocyclic.

Keywords: Finite groups, Posets, Subgroup complexes, Upper intervals, Automorphisms.

Remerciements

Comme le veut la coutume, l'auteur a la lourde tâche de procéder aux remerciements des personnes qui ont contribué d'une manière ou d'une autre à la réalisation de ce travail. Je n'ai pas l'intention de me soustraire à cet exigeant devoir, même si quelques lignes maladroitement rédigées ne peuvent que faiblement rendre honneur aux personnes citées ci-dessous et à tout ce qu'elles m'ont apporté, que ce soit sur le plan mathématique ou personnel.

Pour commencer, je voudrais bien entendu remercier chaleureusement mon directeur de thèse, le professeur Jacques Thévenaz, qui a rempli ce rôle à merveille et qui a eu beaucoup de patience pour écouter et décoder mes explications parfois brouillonnes et imprécises. Je le remercie aussi pour l'énorme travail de relecture et de correction qu'il a effectué avec énormément de soin et d'encre rouge.

Mes remerciements vont aussi aux membres du jury qui ont accepté de lire et d'évaluer ce travail, ainsi que pour leurs commentaires pertinents. Je remercie tout particulièrement le professeur Serge Bouc dont les compétences en GAP ont été particulièrement utiles pour détecter une faute dans la version initiale du Chapitre 3.

Ces années de travail auraient pu manquer de saveur sans la présence de nombreux collègues avec qui j'ai eu l'occasion de partager énormément de pauses-café, accompagnées quelque fois de discussions mathématiques et très souvent de chocolat. Spéciale dédicace donc aux personnes suivantes (par ordre d'apparition à l'écran): Muriel et Jérôme (mention spéciale à vous deux), Jean-Marie, Jean, Giordano, Vince, Manu, Caroline, Arianna, Lucile, Paul, Donna, Christine, Mélanie, Jean-Baptiste, Maria et tous les autres...

Un tout grand merci aussi à mes parents pour m'avoir permis de commencer des études et qui ne se rendaient certainement pas compte du temps que ça prendrait pour les terminer ... Un immense merci à ma femme, Teha'amana, qui m'a beaucoup soutenu et qui supporte toujours avec beaucoup de patience mes bavardages mathématiques.

Et finalement, un tout grand merci à .... (à compléter avec votre nom, si j'ai oublié de vous mentionner ci-dessus).

Le silence qui accompagnera le moment où vous tournerez cette page est dédié à la mémoire de Michel Matthey.

Contents

Introduction

With no surprise, the purpose of this introduction is to give an outline of the content of this work. We have chosen however to give detailed introductions at the beginning of each chapter and for this reason we will stay at a very general level for the present introduction.

Let us give here two words of warning. Firstly, this work takes place in the study of finite groups and even if some of the following considerations may be valid for infinite groups, we will not consider them. From now on "group" always has to be understood as "finite group". Secondly, throughout this work, p will always denote a prime number. In general, p may be even, but there will be however some situations in which we will have to assume that p is odd. In this case, this will be explicitly written at the beginning of the corresponding section.

The importance of group theory in mathematics as well as in other scientific disciplines suffers no contradiction. Anyone with basic notions in group theory is certainly aware that p-groups in turn play a central role in the study of finite groups. The role of extraspecial p-groups in representation theory and cohomology of groups is perhaps less known. It may well be that the reader does not even know what an extraspecial p-group is. He will hopefully have the occasion to fill in this gap in his knowledge by reading this work. The reader already familiar with extraspecial p-groups can refer to the introduction of Benson and Carlson's paper [3] for references to theorems and problems whose resolution depends heavily on the extraspecial case.

One of the interesting features of extraspecial p-groups is that their *central quotient*, that is, the quotient of the group by its center, has the structure of a vector space over the field $\mathbb{F}_p$ with p elements, and carries a natural geometry coming from the commutators and the p-th powers of elements of the group. The word "geometry" refers here to a symplectic or orthogonal geometry. The impatient reader is referred to the introduction of Chapter 1 for more details. For the others, let us just say that this geometry can be used effectively to gain many informations on the group itself. It is, for instance, possible to use this geometry to classify extraspecial p-groups. In another direction, Winter showed in [32] how to compute the automorphism groups of extraspecial p-groups, mainly in term of subgroups of symplectic or orthogonal groups.

There are other groups for which such a geometry can be defined and one of the main purposes of Chapter 1 is to review and generalize these constructions mainly for the following two classes of groups:

(I) p-groups with a cyclic and central Frattini subgroup.

(II) p-groups of class 2 with a cyclic center and a homocyclic central quotient.

Similarly to the case of extraspecial p-groups, these groups are determined by the geometry carried by their central quotient. Note however that for the p-groups in (II), we leave the setting of vector spaces and have to consider free modules over rings $\mathbb{Z}/p^m\mathbb{Z}$ instead. An other purpose of Chapter 1 is to give classifications in some classes of p-groups of class 2, including (I) and (II).

The first part of Section 1.3 is dedicated to the classification of the p-groups in (I), that is, with a cyclic and central Frattini subgroup. Without too much additional work, this classification can be used to classify all p-groups with a cyclic (not necessarily central) Frattini subgroup. This is done in a second part of Section 1.3.

We begin Section 1.4 with the construction of the geometry on the central quotient of any p-group of class 2 with a cyclic center (note that we don't require the central quotient to be homocyclic). As a second step, we use this geometry to classify the p-groups in (II), that is, with homocyclic central quotient. As a third and last step, we show how this can be used to classify all p-groups of class 2 with a cyclic center. For all this, we will however assume that p is odd and we end up Section 1.4 with remarks on the case $p = 2$.

All the classifications obtained in Chapter 1 have been known for a long time, although the original proofs rely generally on a different approach. The interest of Chapter 1 lies thus in the method, that uses as much as possible the geometry on the central quotient, rather than in the results obtained. This method can be considered to be relatively standard for p-groups with a cyclic and central Frattini subgroup, but as far as we know, it has not been used previously for p-groups of class 2 with cyclic center. It is in this latter context that our work has the most interest and this for the following two reasons. Firstly, this throws some light on the classification, especially in the case of a homocyclic central quotient. Secondly, this will also allow us to describe the automorphism groups of p-groups of class 2 with a cyclic center and a homocyclic central quotient, at least for p odd.

The second chapter is concerned with what was initially the main topic of this thesis, namely the study of *subgroup complexes*, that is, simplicial complexes arising from partially ordered sets (poset for short) consisting of subgroups of a given group, ordered by inclusion. The study of subgroup complexes seems to go back to Brown [10], who introduced the poset $\mathcal{S}_p(G)$ of all non-trivial p-subgroups of a given group G for a fixed prime p. A great impulsion was given shortly afterwards by Quillen in [23], where he introduces in particular the poset $\mathcal{A}_p(G)$ of all non-trivial elementary abelian subgroups of the group G. Since then, many other subgroup complexes have been defined and studied and one of these, namely the poset $\mathcal{A}_p(P)_{\geq 2}$, has proved to be of particular interest in representation theory and more precisely for the study of endotrivial modules. As the notation suggests, this poset $\mathcal{A}_p(P)_{\geq 2}$ is defined as the poset of all elementary abelian p-subgroups of P of rank at least 2. For more on subgroup complexes, the reader can refer to [31] or [2, Chapter 6].

A great part of Chapter 2 is concerned with the study of the posets $\mathcal{A}_p(P)_{\geq 2}$. In [8], Bouc and Thévenaz showed that this poset is homotopy equivalent to a wedge of spheres. In Section 2.3, we will use Bouc and Thévenaz's work to compute explicitly the number and the dimension of the spheres occurring in the homotopy type of $\mathcal{A}_p(P)_{\geq 2}$, when P is a p-group with cyclic derived subgroup. This can be easily reduced to the case of p-groups with a cyclic Frattini subgroup, and the classifications obtained in Chapter 1 will thus prove especially useful in this context.

In Section 2.5, we consider all p-groups with a cyclic derived subgroup and determine precisely for which of these groups the poset $\mathcal{A}_p(P)_{\geq 2}$ is homotopically Cohen-Macaulay.

Section 2.4 contains three general results on the maximal dimension that a sphere occurring in $\mathcal{A}_p(P)_{\geq 2}$ may have. More precisely, the first result is an upper bound, depending on the order of the group P, for the homological dimension of $\mathcal{A}_p(P)_{\geq 2}$. In the two other results, we show that this bound can be reached and give information on the p-groups for which this bound is reached.

Another part of Chapter 2 is concerned with upper intervals in $\mathcal{A}_p(P)$, namely the posets $\mathcal{A}_p(P)_{>A}$ consisting of all elementary abelian subgroups of P strictly containing some fixed elementary abelian subgroup $A \in \mathcal{A}_p(P)$. These posets are studied in Section 2.7, where our purpose is to generalize the work of Bouc and Thévenaz by using a spectral sequence introduced by Quillen in [23]. The terms appearing in this spectral sequence are homology groups with non-constant coefficients and Section 2.6 is here to recall the definition of these groups. We derive also in Section 2.6 another spectral sequence given in terms of standard homology groups and converging to the homology groups with non-constant coefficients. With all this put together, we can derive a spectral sequence E^1_{rs} converging to the homology groups of $\mathcal{A}_p(P)_{>A}$. The terms of this spectral sequence are given mostly as upper intervals in $\mathcal{A}_p(P)_{>A}$. There are however, in addition to the problem of handling differentials, some terms that we are not able to describe reasonably well, unless in some special situations.

We end up Chapter 2 with Section 2.8, in which we give some considerations concerning the work of Fumagalli on the posets $\mathcal{A}_p(G)$ for solvable groups G. He claims in [12], that for a solvable group G, the poset $\mathcal{A}_p(G)$ is always homotopy equivalent to a wedge of spheres. His proof relies however on a result that turns out to be false. The main purpose of Section 2.8 is to give counterexamples to this particular result and to show how this affects the rest of Fumagalli's paper.

The third and last chapter is concerned with the study of automorphism groups of some p-groups of class 2. We will first expand Winter's work, in order to describe the automorphism groups of p-groups with a cyclic and central Frattini subgroup. We can then use these results to describe the automorphism groups of all p-groups with a cyclic Frattini subgroup. We end up Chapter 3 with the description of automorphism groups of odd order p-groups of class 2 with a cyclic center and a homocyclic central quotient.

In addition to these three chapters, the reader will find also two appendices. The first one contains a brief survey of non-degenerate alternating forms on vector spaces over the field $\mathbb{F}_p$ and generalizations to the setting of $\mathbb{Z}/p^m\mathbb{Z}$-modules.

In Chapter 3, we make use, at a certain point, of a particular property of the orthogonal group $O(2n+1, 2)$. We have not been able to find this property, nor a proof of it, anywhere else. We have thus included a proof of this property in this work and this is the content of our second appendix.

Chapter 1

Classifications

In this chapter we classify some classes of p-groups of class 2. Our first main result is a classification of p-groups with cyclic Frattini subgroup. Our second main result is a classification of p-groups of class 2 with cyclic center and such that the quotient group $P/Z(P)$ is homocyclic. For p odd, we will also show some results when $P/Z(P)$ is not homocyclic. The real interest of this chapter does not lie in the results, which have been known for a long time, but rather in the method which uses as much linear algebra as possible. This allows us to give a uniform and conceptual treatment of these various classifications. This will be of particular interest in the study of automorphism groups that we will perform in Chapter 3.

1.1 Introduction

If G is a group, we will denote indistinctively G' or $[G,G]$ its derived subgroup, that is, the subgroup of G generated by all the commutators $[x,y] = xyx^{-1}y^{-1}$ for $x, y \in G$. If z is an element of the center $Z(G)$ of G, then one has rather directly that $[xz, y] = [x, y] = [x, yz]$. For any central subgroup H of G, there is thus a well-defined map

$$b : G/H \times G/H \to G',$$

given by $b(\overline{x}, \overline{y}) = [x, y]$, where we use $\bar{\cdot}$ to denote the class of an element of G in G/H. It follows directly from the definition that $b(\overline{x}, \overline{x}) = 1$ for all $x \in G$, and if $b(\overline{x}, \overline{y}) = 1$ for all $\overline{y} \in G/Z(G)$, then $x \in Z(G)$.

We suppose from now on that G' is contained in H, so that in particular G' as well as G/H are abelian groups. We also have that $G' \leq Z(G)$ and an easy calculation shows that

$$\begin{aligned} b(\overline{x}_1\overline{x}_2, \overline{y}) &= b(\overline{x}_1, \overline{y})b(\overline{x}_2, \overline{y}), \text{ for all } x_1, x_2, y \in G; \\ b(\overline{x}, \overline{y}_1\overline{y}_2) &= b(\overline{x}, \overline{y}_1)b(\overline{x}, \overline{y}_2), \text{ for all } x, y_1, y_2 \in G. \end{aligned}$$

If we denote G' and G/H additively, we can rewrite the above information in the following way:

$$b(v,v) = 0, \text{ for all } v \in G/H. \tag{1.1}$$
$$\text{If } b(v,w) = 0 \text{ for all } w \in G/H, \text{ then } v \in Z(G)/H. \tag{1.2}$$
$$b(v_1 + v_2, w) = b(v_1, w) + b(v_2, w), \text{ for all } v_1, v_2, w \in G/H. \tag{1.3}$$
$$b(v, w_1 + w_2) = b(v, w_1) + b(v, w_2), \text{ for all } v, w_1, w_2 \in G/H. \tag{1.4}$$

These equations show that, in some sense, b is a bilinear alternating form on $V = G/H$ with $V^{\perp} = Z(G)/H$. But for this to be precise, one needs to have a compatible linear structure on G/H and G', namely G' should be isomorphic to some ring R and G/H should be an R-module. The first reasonable situation that comes in mind is the setting of vector spaces, that is, G' would be isomorphic to some field $\mathbb{F}$ and G/H would have the structure of an $\mathbb{F}$-vector space. Let us give an example to illustrate how such a situation can happen.

Example 1.1.1. Let p be a prime and suppose that $G = P$ is a non-abelian p-group with cyclic center and that $H = \Phi(P)$ is contained in $Z(P)$. Here $\Phi(P)$ denotes the Frattini subgroup of P, that is, the subgroup of P generated by all commutators and p-th powers in P. In this situation, the quotient group $V = P/\Phi(P)$ is abelian and has exponent p, hence can be viewed as a vector space over the field $\mathbb{F}_p$ with p elements. We will show in Section 1.3 that under these assumptions we have furthermore that P' has order p, hence can be identified with the field $\mathbb{F}_p$ once a generator is chosen. With these identifications, the map $b : V \times V \to \mathbb{F}_p$ can be seen as an alternating form, in the usual sense, on the $\mathbb{F}_p$-vector space V with $V^{\perp} = Z(P)/\Phi(P)$.

The theory of alternating forms is rather standard, at least for vector spaces, so that once b is seen to be an alternating form, a lot of information is available on the group G/H and this information can be lifted to G. One of the aims of this chapter is to show how this map b can be used to gain information on the structure of the group. We will in particular show how it can be used to classify some classes of p-groups.

Section 1.3 is dedicated to p-groups with a cyclic Frattini subgroup. The main result of this section is a classification of these groups. As a first step, we will consider the p-groups of Example 1.1.1, that is, p-groups with a cyclic center and a central Frattini subgroup. For such groups, that we will call from now on quasi-extraspecial p-groups, we will make more precise the construction of the alternating form b on $P/\Phi(P)$. We will also define a map $\varphi : V \to \mathbb{F}_p$ induced by taking p-th powers. We will show that this map is linear, unless $p = 2$ and $|\Phi(P)| = 2$ in which case φ will be a quadratic form with polar form given by the alternating form b induced by the commutators. Dealing with commutators in P is done via the alternating form b and p-th powers are controlled via the map φ. This will allow us to describe and classify quasi-extraspecial p-groups.

As a second step, we will consider p-groups with a cyclic and central Frattini subgroup, but this time the center is not supposed to be cyclic anymore. We will show that these groups are direct products of a quasi-extraspecial p-group with an elementary abelian p-group. This gives a classification of p-groups with a cyclic and central Frattini subgroup, and it remains to consider p-groups with a Frattini subgroup cyclic but not central. This will be done in a second part of Section 1.3 and we will see that this situation can happen only for $p = 2$.

Putting all the results together gives a classification of all p-groups with a cyclic Frattini subgroup.

In Section 1.4, we will see that the situation is relatively similar for odd order p-groups P of class 2 with a cyclic center and such that the abelian group $P/Z(P)$ is homocyclic of type p^m, for some $m \geq 1$. In this situation, the quotient group $V = P/Z(P)$ can be viewed as a regular alternating space over the ring $\mathbb{Z}/p^m\mathbb{Z}$. Taking p^m-th powers induces a linear map on V and this will allow us to give a complete description of these groups. We will go then a step further and give a description of all odd order p-groups of class 2 with a cyclic center. In Section 1.4, we will focus mainly on the case p odd, but we will also give some results when $p = 2$, especially in the homocyclic case.

1.2 Preliminaries on p-groups

In this section we review some basic definitions and results in finite group theory. We assume that the reader already has a basic knowledge of group theory and this section is here to stress some facts that will be important in this work. For more details, the reader can refer to standard textbooks such as [14], [1], or [26] and [27]. In all cases, the reader is advised to read at least the results on commutators and especially Lemma 1.2.1 and Lemma 1.2.2.

Abelian p-groups and rank

We will denote by C_k a cyclic group of order k. Recall that if P is an abelian p-group there exists an integer $n \geq 1$ and integers $e_1, \ldots, e_n$ with $e_i \geq 1$ such that P is isomorphic to the direct product of the cyclic groups $C_{p^{e_i}}$. The integer n and the integers e_i are uniquely determined up to isomorphism and we say that P has *type* $(p^{e_1}, \ldots, p^{e_n})$. An abelian p-group is *homocylic* of type p^e if $e_i = e$ for all $i = 1, \ldots, n$.

If an abelian group E is homocyclic of type p, then E is called *elementary abelian*. A p-group E is elementary abelian if and only if E is abelian and has exponent p. It is important to remind that such a group can always be seen as a vector space over the field $\mathbb{F}_p$ with p elements (see [14, Theorem 1.3.2]).

Let E be an elementary abelian p-group. The *rank* of E is the integer $\mathrm{rk}(E)$ defined as the dimension of E as a vector space over $\mathbb{F}_p$. For an arbitrary group G, the *p-rank* of G is defined as the maximum of the rank of E, as E ranges over all elementary abelian p-subgroups of G. If G is an arbitrary group we will denote $r_p(G)$ the p-rank of G. However, if P is a p-group, we will preferably use the notation $\mathrm{rk}(P)$ for the p-rank of P.

Commutators

Let G be a (finite) group. We will denote by $Z(G)$ its center and recall from the introduction that we denote by G' as well as $[G, G]$ its *derived subgroup*, that is, the subgroup of G generated by all *commutators* $[x, y] = xyx^{-1}y^{-1}$. When the commutators are central, they satisfy very useful properties that we will often use implicitly in the remainder of this work. In the course of a proof, if an argument involving commutators is not clear for the reader, he should refer first to the two following lemmas.

Lemma 1.2.1. *If G is a group with $G' \leq Z(G)$, then*

a) $[x_1x_2, y] = [x_1, y][x_2, y]$*, for all* $x_1, x_2, y \in G$*;*

b) $[x, y_1y_2] = [x, y_1][x, y_2]$*, for all* $x, y_1, y_2 \in G$*.*

Proof. Part a) follows from the following elementary calculation and part b) is proved similarly.

$$[x_1x_2, y] = x_1x_2yx_2^{-1}x_1^{-1}y^{-1} = x_1(x_2yx_2^{-1}y^{-1})yx_1^{-1}y^{-1} = [x_1, y][x_2, y].$$

□

Lemma 1.2.2. *Let G be a group and let $x, y \in G$ such that $[x, y]$ commutes with x and y. Then*

a) $[x, y]^k = [x^k, y] = [x, y^k]$*;*

b) $(xy)^k = x^ky^k[y, x]^{\frac{1}{2}k(k-1)}$*, for all* $k \in \mathbb{Z}$*.*

Proof. See Lemma 2.2.2 in [14]. □

Frattini subgroup

Let p be an arbitrary prime and let P be a p-group. For $n \geq 1$, we denote by $\Omega_n(P)$ the subgroup generated by all elements of order at most p^n. We denote by $\mho^n(P)$ the subgroup generated by all p^n-th powers of elements of P.

For an arbitrary group G, the Frattini subgroup $\Phi(G)$ of G is defined as the intersection of all maximal subgroups of G. For a p-group P, there is a more accurate characterization of the Frattini subgroup that we will take as a definition, namely it is the smallest normal subgroup of P with elementary abelian quotient.

Definition 1.2.3. The Frattini subgroup $\Phi(P)$ of a p-group P is the subgroup generated by $[P, P]$ and $\mho^1(P)$.

We would like to point out some elementary facts concerning these subgroups that we will sometimes use implicitly.

Remark 1.2.4.

a) If H is one of the subgroups $Z(P)$, $\Phi(P)$, $[P, P]$, $\Omega_n(P)$ or $\mho^n(P)$, then H is characteristic in P, and in particular, $H \cap Z(P) \neq 1$ if $H \neq 1$.

b) If a subgroup H of a p-group P contains P', then H is normal in P. Consequently, all subgroups of P containing $\Phi(P)$ are normal in P.

c) If P is a p-group and $\Phi(P)$ is maximal in P, then P is cyclic.

Central products

Let G_1 and G_2 be groups and let Z_1, respectively Z_2, be a central subgroup of G_1, resp. G_2. Suppose that the two subgroups Z_1 and Z_2 are isomorphic. Given an isomorphism $\theta : Z_1 \to Z_2$, one can form the *central product* $G_1 * G_2$ of G_1 and G_2 with respect to Z_1, Z_2 and θ. More precisely, $G_1 * G_2$ is defined as the quotient of $G_1 \times G_2$ by the normal subgroup $\{(z_1, \theta(z_1)^{-1}) \mid z_1 \in Z_1\}$ (see for example Section 2.5 in [14] for more details). It is important to note that, contrary to what the notation suggests, the group $G_1 * G_2$ depends on the choice of the subgroups Z_1, Z_2 and on the choice of the isomorphism between them.

In this work, we will only encounter central products on groups with cyclic center and in this situation, the central subgroups are completely determined by their order. Therefore, if G_1 and G_2 have cyclic center, we will write $G_1 \underset{C_r}{*} G_2$ for the central product of G_1 and G_2 relatively to the unique subgroups of $Z(G_1)$ and $Z(G_2)$ of order r. Of course, for this definition to be complete we need to make explicit the chosen isomorphism. However, there are situations in which the central product does not depend on the chosen isomorphism.

Lemma 1.2.5. *Let G_1, G_2 be groups and let Z_1, respectively Z_2, be a central subgroup of G_1, resp. G_2. Suppose that Z_1 and Z_2 are isomorphic and suppose that any automorphism of Z_1 is the restriction of an automorphism of the whole group G_1. Then the central products $G_1 * G_2$ relatively to any isomorphism between Z_1 and Z_2 are all isomorphic.*

The central product is symmetric, that is, $G_1 * G_2$ is canonically isomorphic to $G_2 * G_1$. It satisfies also some condition of associativity. Let G_1, G_2, G_3 be groups with subgroups $Z_1 \leq Z(G_1)$, $Z_2', Z_2'' \leq Z(G_2)$ and $Z_3 \leq G_3$ and such that $Z_1 \cong Z_2'$ and $Z_2'' \cong Z_3$. The subgroup Z_2'' can be identified canonically with a central subgroup in the central product $(G_1 * G_2)$ with respect to Z_1 and Z_2'. The subgroup Z_3 is thus isomorphic to a central subgroup of $G_1 * G_2$ and one can form the central product $(G_1 * G_2) * G_3$. In a similar manner, one can form also the central product $G_1 * (G_2 * G_3)$ and it turns out that these two groups are isomorphic. As a consequence, the parentheses can be omitted in this situation.

Let G be a group and Z a central subgroup of G. One can form the central product $G * G$ with respect to the identity on Z. For $\ell > 1$, we will denote $G^{*\ell}$ the central product $G^{*(\ell-1)} * G$ with the convention that $G^{*1} = G$ and G^{*0} is the trivial group.

Semi-direct product

If G is a group and A is a subgroup of the automorphism group $\mathrm{Aut}(G)$ of G, one can form the *semi-direct product* $G \rtimes A$ of A acting on G. Both G and A can be identified with subgroups of $G \rtimes A$ and we will use the convention that under these identifications $aga^{-1} = a(g)$ for all $a \in A$ and $g \in G$.

If α is an automorphism of G of some order k, we will denote $G \rtimes_\alpha C_k$ the semi-direct product of the subgroup of $\mathrm{Aut}(G)$ generated by α acting on G. When this leads to no confusion, we will sometimes omit the subscript α.

In this work, many groups will be described as semi-direct products, so let us recall next some standard results on automorphism groups, especially for cyclic p-groups.

Automorphisms of p-groups

If E is an elementary abelian p-group, then the automorphism group of the group E is the same as the group of all invertible linear transformations of E viewed as an $\mathbb{F}_p$-vector space. If n denotes the rank of E, then $\mathrm{Aut}(E)$ can be identified with the group $GL_n(\mathbb{F}_p)$. For cyclic p-groups, the following information on the structure of the automorphism groups is available.

Lemma 1.2.6. *Let $P = \langle x \rangle$ be a cyclic p-group of order p^{m+1}, $m \geq 1$.*

a) If $p = 2$ and $m = 1$, then $\mathrm{Aut}(P)$ is cyclic of order 2 generated by $x \mapsto x^{-1}$.

b) If $p = 2$ and $m > 1$, then $\mathrm{Aut}(P)$ is an abelian 2-group of type $(2^{m-1}, 2)$ with basis $x \mapsto x^5$ and $x \mapsto x^{-1}$.

c) If p is odd, $\mathrm{Aut}(P)$ is cyclic of order $p^m(p-1)$ and a Sylow p-subgroup of $\mathrm{Aut}(P)$ is cyclic with generator $x \mapsto x^{1+p}$.

Proof. See for example Lemma 5.4.1 in [14]. □

Corollary 1.2.7. *Let $P = \langle x \rangle$ be a cyclic p-group of order p^{m+1}, $m \geq 1$, and let $A = \mathrm{Aut}(P)$.*

a) If $p = 2$ and $m > 1$, then $\Omega_1(A)$ is elementary abelian of rank 2 with basis given by $x \mapsto x^{1+2^m}$ and $x \mapsto x^{-1}$.

b) If p is odd and S_p is the Sylow p-subgroup of A, then $\Omega_1(S_p)$ is cyclic of order p and generated by $x \mapsto x^{1+p^m}$.

Proof. See for example Corollary 5.4.2 in [14]. □

Some standard p-groups

We recall finally notation and definitions of some p-groups that will appear constantly in this work. Recall first that if p is a prime, there are exactly two non-abelian p-groups of order p^3. When $p = 2$, they are the *dihedral group* D_8 and the *quaternion group* Q_8. When p is odd, we will denote by X_{p^3}, respectively $X^-_{p^3}$, the non-abelian group of order p^3 and exponent p, resp. p^2. The group X_{p^3} can be defined as the group $U_3(\mathbb{F}_p)$ of all upper triangular matrices with entries 1 on the diagonal. The group $X^-_{p^3}$ can be defined as the semi-direct product of a cyclic group of order p acting on a cyclic group of order p^2 with generator y, with respect to the automorphism sending y to y^{1+p}.

We will call X_{p^3} and D_8 extraspecial groups of *type I*. The groups $X^-_{p^3}$ and Q_8 will be called extraspecial groups of *type II*. These groups have the following presentations:

$$X_{p^3} = \langle x, y \mid x^p = y^p = 1, [x,y]^p = 1, [x,[x,y]] = [y,[x,y]] = 1 \rangle.$$

$$X^-_{p^3} = \langle x, y \mid x^p = 1, y^p = [x,y], [x,y]^p = 1, [x,[x,y]] = [y,[x,y]] = 1 \rangle.$$

$$D_8 = \langle x, y \mid x^2 = y^2 = 1, [x,y]^2 = 1, [x,[x,y]] = [y,[x,y]] = 1 \rangle.$$

$$Q_8 = \langle x, y \mid x^2 = y^2 = [x, y], [x, y]^2 = 1, [x, [x, y]] = [y, [x, y]] = 1 \rangle.$$

For $m > 1$, we will denote respectively by $D_{2^{m+2}}$, $SD_{2^{m+2}}$ and $Q_{2^{m+2}}$ the dihedral, semi-dihedral and quaternion group of order 2^{m+2}. These groups have the following presentations:

$$D_{2^{m+2}} = \langle x, y \mid x^2 = y^{2^{m+1}} = 1, [x, y] = y^{-2} \rangle.$$

$$SD_{2^{m+2}} = \langle x, y \mid x^2 = y^{2^{m+1}} = 1, [x, y] = y^{-2+2^m} \rangle.$$

$$Q_{2^{m+2}} = \langle x, y \mid x^4 = 1, y^{2^m} = x^2, [x, y] = y^{-2} \rangle.$$

Note that $[x, y] = y^{-2}$ means that x acts on y as the automorphism sending y to y^{-1}. Similarly, $[x, y] = y^{-2+2^m}$ means that x acts on y as the automorphism sending y to y^{-1+2^m}.

For an arbitrary prime p and $m > 1$, we denote $M_{p^{m+2}}$ the semi-direct product of a cyclic group of order p acting on a cyclic group of order p^{m+1} generated by y, with respect to the automorphism sending y to y^{1+p^m}. This group has the following presentation:

$$M_{p^{m+2}} = \langle x, y \mid x^p = y^{p^{m+1}} = 1, [x, y] = y^{p^m} \rangle.$$

Remark 1.2.8.

a) In the above notation, the index, namely p^3, 8, 2^{m+2} or p^{2m+2} , represents the order of the group and the parameter m, which equals 1 by convention when the group has order 8 or p^3, is the p-valuation of the order of the Frattini subgroup.

b) The definition of the group $M_{p^{m+2}}$ also makes sense for $m = 1$ and we draw the attention of the reader to the fact that M_{p^3} is the group $X^-_{p^3}$ when p is odd, whereas M_{2^3} is isomorphic to D_8.

c) For $m > 1$, the group $Q_{2^{m+2}}$ is sometimes called the *generalized* quaternion group of order 2^{m+2}. To make the text more readable, we have chosen not to use the adjective "generalized".

To close these preliminaries, we give a last result that concerns p-groups containing a maximal cyclic subgroup. For the proof, the reader can refer to [14, Theorem 5.4.4].

Lemma 1.2.9. *Let P be a non-abelian p-group of order p^{m+2}, $m \geq 1$, which contains a cyclic subgroup of order p^{m+1}. Then*

a) If p is odd and $m = 1$, then P is isomorphic to $X^-_{p^3}$.

b) If p is odd and $m > 1$, then P is isomorphic to $M_{p^{m+2}}$.

c) If $p = 2$ and $m = 1$, then P is isomorphic to D_8 or Q_8.

d) If $p = 2$ and $m > 1$, then P is isomorphic to $M_{2^{m+2}}$, $D_{2^{m+2}}$, $Q_{2^{m+2}}$ or $SD_{2^{m+2}}$.

1.3 Classification of p-groups with a cyclic Frattini subgroup

Definitions and first properties

To begin this section, we recall some more or less known facts concerning the special case of p-groups with Frattini subgroup of order p. This allows us to make a quick tour of some terminology that can be found in the literature and to introduce some notation that we will use throughout this text.

If P is a non-abelian p-group with $Z(P) = \Phi(P)$ of order p, then it is standard to call P an *extraspecial p-group.* It is well known that an extraspecial p-group has order $p^{2\ell+1}$ for some $\ell \geq 1$, and that there are exactly two non-isomorphic extraspecial p-groups of the same order. When p is odd, these two groups are determined by their exponent and we will denote by $X_{p^{2\ell+1}}$, respectively $X^-_{p^{2\ell+1}}$, the extraspecial p-group of order $p^{2\ell+1}$ and exponent p, resp. p^2. We make two small remarks to show how these groups can be obtained from what we already know. The reader can take this as a definition.

Remark 1.3.1.

a) The group $X_{p^{2\ell+1}}$ is isomorphic to a central product $(X_{p^3})^{*\ell}$ and the group $X^-_{p^{2\ell+1}}$ is isomorphic to a central product $(X_{p^3})^{*(\ell-1)} * X^-_{p^3}$, where X_{p^3} and $X^-_{p^3}$ are the two non-abelian p-groups of order p^3 defined previously.

b) It can be useful to think of the group $X_{p^{2\ell+1}}$ as the subgroup P of $U_{\ell+2}(\mathbb{F}_p)$ consisting of matrices of the following form:

$$\begin{pmatrix} 1 & * & \cdots & * \\ & \ddots & 0 & \vdots \\ & 0 & \ddots & * \\ & & & 1 \end{pmatrix}$$

To connect this definition with the preceding remark, let I denote the identity matrix and let e_{ij} be the elementary matrix with 1 in the (i, j)-th entry and 0 elsewhere. For $1 < j < \ell + 2$, let H_j be the subgroup of P generated by $I + e_{1,j}$ and $I + e_{j,\ell+2}$. For $1 < j, k < \ell + 2$, an elementary calculation shows that

$$[I + e_{1,j}, I + e_{k,\ell+2}] = I + \delta_{j,k} e_{1,\ell+2}.$$

Similarly,

$$[I + e_{1,j}, I + e_{1,\ell+2}] = [I + e_{\ell+2,k}, I + e_{1,\ell+2}] = 0, \text{ for } 1 < j, k < \ell + 2.$$

As a consequence, for all $1 < j < \ell + 2$, the center of H_j is generated by $I + e_{1,\ell+2}$, the group H_j is isomorphic to X_{p^3} and H_j commutes with H_k for all $k \neq j$. It follows that $P = H_1 * \cdots * H_\ell$, hence is a central product of ℓ copies of the group X_{p^3}.

c) If P is the group X_{p^3} or the group $X^-_{p^3}$, then any automorphism of $Z(P)$ is the restriction of an automorphism of the whole group P, so that the central products $(X_{p^3})^{*\ell}$ and $(X_{p^3})^{*(\ell-1)} * X^-_{p^3}$ do not depend on how the amalgamation is made along the centers. Let us show briefly how an automorphism of the center can be extended to an automorphism of P. If P is the group X_{p^3}, then P is generated by two elements x and y of order p and the center of P is generated by $z = [x, y]$. An automorphism α of $Z(P)$ is given by $\alpha(z) = z^k$, for some k prime to p. The automorphism α can be extended to an automorphism $\tilde{\alpha}$ of P by defining $\tilde{\alpha}$ on the generators of P by

$$\tilde{\alpha}(x) = x^k \text{ and } \tilde{\alpha}(y) = y.$$

An easy calculation shows that all the relations defining P are preserved, so that $\tilde{\alpha}$ extends to a endomorphism of P. This endomorphism is also bijective, since k is prime to p.

When $p = 2$, the two extraspecial 2-groups of order $2^{2\ell+1}$ are the two groups $D_8^{*\ell}$ and $D_8^{*(\ell-1)} * Q_8$. To be coherent with our previous notation, we will denote these two groups respectively by $X_{2^{2\ell+1}}$ and $X^-_{2^{2\ell+1}}$.

For any prime number $p \geq 2$, we will refer to $X_{p^{2\ell+1}}$, respectively $X^-_{p^{2\ell+1}}$, as the *extraspecial p-group of type I*, respectively *type II*, and order $p^{2\ell+1}$.

A non-abelian p-group with a Frattini subgroup cyclic of order p and with a center cyclic of order p^2 is often referred to as an *almost extraspecial p-group*. These groups arise as the central product of an extraspecial p-group of type I and a cyclic group of order p^2.

The non-abelian p-groups with a Frattini subgroup of order p have been called *generalized extraspecial* by Stancu [25]. However, it seems that this terminology has not been used elsewhere for the moment. In [25], Stancu shows that these groups are direct products of an elementary abelian p-group with either an extraspecial p-group, or an almost extraspecial p-group.

For the more general case of p-groups with a Frattini subgroup cyclic but with arbitrary order, one has the two following terminologies.

A p-group is said to be of *symplectic type* if it has no non-cyclic characteristic abelian subgroups. Such groups can be written as a central product $X * S$ where either X is extraspecial, or $X = 1$, and either S is cyclic, or S is dihedral, semi-dihedral or quaternion, and of order 2^{m+2} with $m > 1$.

Newman introduced in [21] the class of *JN2-groups* ("just nilpotent-of-class-2 groups"). These groups may be infinite, but when finite they correspond to p-groups with cyclic center and central Frattini subgroup. In his paper, Newman gives a classification of these groups, based on the non-degenerate alternating form induced by commutators. We will use the same method in this section, but we will consider in addition the linear form induced by taking p-th powers.

The classification in the general case of p-groups with a cyclic Frattini subgroup can be found in a paper by Berger, Kovács and Newman [4]. The proof in the case of a central Frattini subgroup is left to the reader and the authors concentrate on the case of a non-central Frattini subgroup.

As the title says, the aim of this section is to classify p-groups with a cyclic Frattini subgroup. The above discussion shows that this classification can already be found in the literature. Our motivation for this section is that we would like to give the most uniform and conceptual treatment possible for these various classifications. For this, we will use the non-degenerate alternating form induced by commutators and the linear form induced by taking p-th powers. This method will have the following two advantages. The first one is that this method can be generalized rather easily for odd order p-groups of class 2 with a cyclic center and this will be done in Section 1.4. The second one is that it makes it possible to describe reasonably well the automorphism groups of some of these groups and this will be done in Chapter 3.

We go on now with some preliminary results and reductions. The following lemma shows that we can easily assume that the center itself is cyclic and this will greatly simplify many arguments.

Lemma 1.3.2. *If P is a non-abelian p-group with a cyclic Frattini subgroup, then $P = Q \times E$, where E is elementary abelian and Q is non-trivial with both $\Phi(Q)$ and $Z(Q)$ cyclic.*

Proof. Let Z denote the elementary abelian subgroup $\Omega_1(Z(P))$. Since P is not abelian, we have that $\Phi(P)$ is non-trivial, so that $\Phi(P) \cap Z(P) \neq 1$, and hence also $\Phi(P) \cap Z \neq 1$. Furthermore, $\Phi(P) \cap Z$ has order p, since $\Phi(P)$ is cyclic. The group Z is elementary abelian, so that we can choose a complement E to $\Phi(P) \cap Z$ in Z, that is,

$$Z = (\Phi(P) \cap Z) \times E. \tag{1.5}$$

Since $P/\Phi(P)$ is elementary abelian, we can find a complement $Q/\Phi(P)$ to $\Phi(P)Z/\Phi(P)$ in $P/\Phi(P)$, that is,

$$P/\Phi(P) = Q/\Phi(P) \times \Phi(P)Z/\Phi(P). \tag{1.6}$$

We show now that $P = Q \times E$ and that Q has the desired properties. Note that (1.6) implies that the group P is generated by Q and $\Phi(P)Z$. But Q contains $\Phi(P)$ and Z itself is generated by E and a subgroup of $\Phi(P)$. Hence, P is generated by Q and E.

Furthermore, (1.6) implies that $Q \cap E$ is contained in $Q \cap \Phi(P)Z = \Phi(P)$, but also $Q \cap E$ is contained in E, so that $Q \cap E$ is contained in $Q \cap (\Phi(P) \cap E) = 1$. We have thus that P is generated by Q and E and that $Q \cap E = 1$, hence $P = Q \times E$, since E is central.

Now, $Q/\Phi(P)$ is elementary abelian, so that $\Phi(Q)$ is contained in $\Phi(P)$, hence is cyclic. Furthermore, $\Omega_1(Z(P)) = \Omega_1(Z(Q)) \times E$, so that $\Omega_1(Z(Q))$ is cyclic of order p. It follows that $Z(Q)$ is cyclic and the lemma is proved. □

Not surprisingly, we will have to make a distinction between the case $p = 2$ and the case p odd. This can be seen in the following Proposition 1.3.5, but let us give first with two elementary, still very useful, lemmas.

Lemma 1.3.3. *Let P be a non-abelian p-group. If $\Phi(P)$ is cyclic and central, then P' has order p.*

Proof. As P' is non-trivial, since P is non-abelian, and contained in the cyclic group $\Phi(P)$, it suffices to show that every element of P' has order p. Since $P' \leq \Phi(P) \leq Z(P)$, Lemma 1.2.2 shows that

$$[x, y]^p = [x^p, y], \text{ for all } x, y \in P.$$

On the other hand, we have $[x^p, y] = 1$, since $x^p \in \Phi(P) \leq Z(P)$, hence $[x, y]^p = 1$ for all $x, y \in P$, and the lemma is proved. □

Lemma 1.3.4. *Let P be a p-group. If $\mho^1(P)$ is cyclic, then there exists $u \in P$ such that $\mho^1(P) = \langle u^p \rangle$.*

Proof. Since x^p is obviously in $\mho^1(P)$, we have $\langle x^p \rangle \leq \mho^1(P)$ for all $x \in P$. If all the subgroups $\langle x^p \rangle$ are strictly contained in $\mho^1(P)$, then all the elements x^p, for $x \in P$, are contained in the unique maximal subgroup of the cyclic group $\mho^1(P)$. Hence, $\mho^1(P) = \langle x^p | x \in P \rangle < \mho^1(P)$, which is a contradiction. There exists thus $u \in P$ such that $\langle u^p \rangle = \mho^1(P)$. □

The proof of the following result can be found along the lines of [4, Theorem 2]. We include it here for the convenience of the reader, but also because it contains many arguments that we will use constantly in this work.

Proposition 1.3.5. *Let p be an odd prime and P a non-abelian p-group. If $\Phi(P)$ is cyclic, then $\Phi(P)$ is central.*

Proof. We prove this proposition by induction on n, where $p^n = |P|$. Note that since P is non-abelian, we must have $n \geq 3$. If $n = 3$, then we must have $|\Phi(P)| = p$, otherwise P would be abelian. It follows immediately that $\Phi(P)$ is central.

Suppose now $n > 3$ and let C_0 denote the centralizer of $\Phi(P)$ in P. Note that $\Phi(P)$, being cyclic hence abelian, is contained in C_0. The p-group P acts on its normal subgroup $\Phi(P)$ by conjugation and this induces an injective homomorphism

$$P/C_0 \hookrightarrow \mathrm{Aut}(\Phi(P)).$$

The quotient group P/C_0 is an elementary abelian p-group, since C_0 contains $\Phi(P)$. Since p is assumed to be odd, the automorphism group of the cyclic p-group $\Phi(P)$ has a cyclic Sylow p-subgroup. Therefore, P/C_0 has order at most p.

If $C_0 = P$ we are done, and we suppose from now on that C_0 has index p in P. In particular, $\Phi(P)$ is strictly contained in C_0, otherwise P would be abelian. Furthermore, $C_0/\Phi(P)$ is obviously elementary abelian, so that we can then choose a subgroup U of C_0 containing $\Phi(P)$ and such that $|U : \Phi(P)| = p$. Remark that U is abelian (it contains $\Phi(P)$ as a maximal central subgroup) and normal in P (it contains P').

Suppose first that there exists such a subgroup U which is cyclic. Now let $x \in P$ and consider its action on U by conjugation. Since $x^p \in \Phi(P)$, then x^p acts trivially on U. It follows that x acts as an automorphism of order 1 or p on the cyclic group U. But then x must act trivially on the subgroup of index p in U, namely $\Phi(P)$. It follows that $\Phi(P)$ is in the center of P.

We suppose now that $\Phi(P)$ is not contained in any cyclic subgroup of P. Remark that in this case we have $\Phi(P) = [P, P]$. We would have otherwise $\Phi(P) = \mho^1(P)$ and $\Phi(P)$ would be strictly contained in a cyclic subgroup of P by Lemma 1.3.4.

We can thus decompose U as $U = A \times \Phi(P)$, with A cyclic of order p. Since A is not contained in $\Phi(P)$, there exists a maximal subgroup L of P which does not contain A. Let $Z = \Omega_1(\Phi(P))$ be the unique cyclic subgroup of order p in $\Phi(P)$.

The subgroups L/Z and AZ/Z intersect trivially and are both normal in P/Z, since L is maximal in P and AZ is actually $\Omega_1(U)$. Furthermore, we can see that these two groups are abelian. This is clear for AZ/Z which is cyclic of order p. Now, $L < P$ and $\Phi(L) \leq \Phi(P)$, so that applying the induction hypothesis to L gives that $\Phi(L)$ is central in L. If L is not abelian, it follows then from Lemma 1.3.3 that $[L, L]$ has order p. If L is abelian, then $[L, L] = 1$. In both cases $[L, L] \leq Z$, showing that L/Z is abelian.

As a consequence, P/Z is the direct product of the two abelian groups L/Z and AZ/Z, so that P/Z is actually abelian. Therefore $Z = [P, P]$ and then $\Phi(P) = [P, P]$ has order p, hence is central, and the proposition is proved. □

Remark 1.3.6. Considering dihedral groups of order 2^{m+2} with $m > 1$, one can see that the above proposition does not hold when $p = 2$.

The p-groups with a cyclic and central Frattini subgroup carry a natural geometry coming from the commutators. This, together with Lemma 1.3.2, motivates the following definition.

Definition 1.3.7. A non-abelian p-group P is called quasi-extraspecial if $Z(P)$ is cyclic and $\Phi(P)$ is central.

Lemma 1.3.2 says in particular that any p-group with a cyclic and central Frattini subgroup is the direct product of a quasi-extraspecial p-group and an elementary abelian p-group. Proposition 1.3.5 shows furthermore that all odd order p-groups with a cyclic Frattini subgroup are direct products of a quasi-extraspecial p-group and an elementary abelian p-group.

Example 1.3.8.

a) Almost extraspecial p-groups are quasi-extraspecial and more generally, central products of the form $X_{p^{2\ell+1}} * C_{p^m}$, for $\ell, m \geq 1$, are quasi-extraspecial.

b) Central products of the form $X_{p^{2\ell+1}} * M_{p^{m+2}}$, for $\ell \geq 0$ and $m \geq 1$, are quasi-extraspecial.

c) Generalized extraspecial p-groups are direct products of a quasi-extraspecial p-group with an elementary abelian p-group.

d) For p odd, non-abelian p-groups of symplectic type are quasi-extraspecial. Note however that there are 2-groups of symplectic type that are not quasi-extraspecial. Consider for example the groups $D_{2^{m+2}}$, $SD_{2^{m+2}}$ and $Q_{2^{m+2}}$, all with $m > 1$.

The alternating form

We will consider that the reader already has a basic knowledge of the theory of alternating forms over vector spaces. Apart from the definitions, we will not use more than the standard result giving the existence of a symplectic basis when the form is non-degenerate. The reader will find some more details in Appendix A.

Let P be a quasi-extraspecial p-group and let

$$b : P/\Phi(P) \times P/\Phi(P) \to [P, P],$$

be defined by $b(\overline{x}, \overline{y}) = [x, y]$.

Lemma 1.3.9. *The map b is well-defined and satisfies the following properties.*

a) $b(\overline{x}_1\overline{x}_2, \overline{y}) = b(\overline{x}_1, \overline{y})b(\overline{x}_2, \overline{y})$ *and* $b(\overline{x}, \overline{y}_1\overline{y}_2) = b(\overline{x}, \overline{y}_1)b(\overline{x}, \overline{y}_2)$.

b) $b(\overline{x}^k, \overline{y}) = (b(\overline{x}, \overline{y}))^k = b(\overline{x}, \overline{y}^k)$.

c) $b(\overline{x}, \overline{x}) = 1$.

Proof. Let $z \in \Phi(P)$. As $\Phi(P) \leq Z(P)$, we have $[xz, y] = [x, y] = [x, yz]$ and thus b is well-defined. Part a) and part b) follow from Lemma 1.2.1 and Lemma 1.2.2 respectively. Part c) is clear since $[x, x] = 1$ for all $x \in G$. □

The quotient $V = P/\Phi(P)$ is elementary abelian, hence can be viewed as a vector space over $\mathbb{F}_p$. Since $\Phi(P)$ is cyclic and central in P by definition, we have from Lemma 1.3.3 that P' has order p. Once a generator of P' is chosen, the group P' can then be identified with the field $\mathbb{F}_p$. With these identifications, $V = P/\Phi(P)$ is a vector space over $\mathbb{F}_p$ and the map b takes its value in $\mathbb{F}_p$.

Corollary 1.3.10. *The map b is an alternating form on the $\mathbb{F}_p$-vector space $V = P/\Phi(P)$. Moreover, $V^\perp = Z(P)/\Phi(P)$.*

Proof. It follows from Lemma 1.3.9 that b is an alternating form. Furthermore, $b(\overline{x}, \overline{y}) = 1$ if and only if $[x, y] = 1$. It follows that $\overline{x} \in V^\perp$ if and only if $x \in Z(P)$. Therefore, $V^\perp = Z(P)/\Phi(P)$. □

Corollary 1.3.11. *If P is a quasi-extraspecial p-group, then the quotient group $P/Z(P)$, viewed as an $\mathbb{F}_p$-vector space, is a non-degenerate alternating space.*

As a consequence, $P/Z(P)$ has order $p^{2\ell}$ for some $\ell \geq 1$, and lifting to P the elements of a symplectic basis of $P/Z(P)$ gives a set of elements $x_1, x_2, \ldots, x_\ell, y_\ell$ of P satisfying the following conditions.

$$P = \langle Z(P), x_i, y_i, i = 1, \ldots, \ell\rangle. \tag{1.7}$$

$$[x_i, y_i] = [x_j, y_j], \text{ for all } 1 \leq i, j \leq \ell. \tag{1.8}$$

$$[x_i, x_j] = [x_i, y_j] = [y_i, y_j] = 1, \text{ for all } 1 \leq i \neq j \leq \ell. \tag{1.9}$$

Definition 1.3.12. Let P be a quasi-extraspecial p-group. A symplectic set of generators for P is a choice of generators $\{x_i, y_j : 1 \leq i \leq \ell\}$ of P satisfying the three above conditions (1.7), (1.8) and (1.9). The elements x_i, y_i, $1 \leq i \leq \ell$ will be called symplectic generators of P.

Remark 1.3.13. If P is quasi-extraspecial and z denotes any element of order p of $Z(P)$, then the symplectic generators can be chosen such that $[x_i, y_i] = z$ for all $i = 1, \ldots, \ell$. This is because the isomorphism between P' and $\mathbb{F}_p$ is given by an arbitrary choice of a generator of P'.

The linear form

Let P be a quasi-extraspecial p-group with $|\Phi(P)| = p^m$. We consider now the map induced by taking p-th powers. We begin with the most natural and standard case of a Frattini subgroup cyclic of order p, that is $m = 1$. In this situation, one has to treat separately the case $p = 2$ and the case p odd. Surprisingly, this distinction disappears totally when $m > 1$. This will become clear in what follows.

Let us suppose first that $m = 1$ and let $\psi : P/\Phi(P) \to \Phi(P)$ be the map given by $\psi(\overline{x}) = x^p$. Note that ψ is well defined since $\Phi(P)$ is cyclic of order p.

Lemma 1.3.14.

a) *For p odd, $\psi(\overline{xy}) = \psi(\overline{x})\psi(\overline{y})$.*

b) *If $p = 2$, $\psi(\overline{xy}) = \psi(\overline{x})\psi(\overline{y})[x, y]$.*

Proof. One the one hand, we have that P' is contained in $\Phi(P)$ which is cyclic of order p, so that $[x, y]^p = 1$ for all $x, y \in P$. On the other hand, for all $x, y \in P$, Lemma 1.2.2 gives

$$(xy)^p = [y, x]^{\frac{1}{2}p(p-1)} x^p y^p. \tag{1.10}$$

When p is odd, $p-1$ is even and thus $[y, x]^{\frac{1}{2}p(p-1)} = ([x, y]^p)^{\frac{p-1}{2}} = 1$. When $p = 2$, the equality (1.10) becomes

$$(xy)^2 = [x, y]x^2y^2 = x^2y^2[y, x] = x^2y^2[x, y].$$

□

Lemma 1.3.15.

a) *For p odd, ψ is a linear form on $P/\Phi(P)$.*

b) *For $p = 2$, ψ is a quadratic form on $P/\Phi(P)$ whose polar form is the alternating form b induced by the commutators.*

We return now to the general situation $m \geq 1$. Recall that $Z(P)$ is cyclic, so that in particular the quotient group $Z(P)/\mho^1(Z(P))$ is cyclic of order p. Furthermore, since $\Phi(P)$ is contained in $Z(P)$, we have $x^p \in Z(P)$ for all $x \in P$, so that we can define a map

$$\varphi : P/\Phi(P) \to Z(P)/\mho^1(Z(P)),$$

by $\varphi(\overline{x}) = \pi(x^p)$, where π is the quotient map $Z(P) \to Z(P)/\mho^1(Z(P))$. The following lemma shows that this map is always linear when $Z(P)$ has order at least p^2. We will see after this lemma what happens when $Z(P)$ has order p.

Lemma 1.3.16. *The map φ is well defined. Furthermore, if $Z(P)$ has order at least p^2, then φ is linear.*

Proof. For $x \in P$ and $z \in \Phi(P) \leq Z(P)$ we have $(xz)^p = x^p z^p$. The map φ is thus well-defined, since $z^p \in \mho^1(Z(P))$.

When p is odd, we have $(xy)^p = x^p y^p$, and thus $\varphi(\overline{xy}) = \varphi(\overline{x})\varphi(\overline{y})$. When $p = 2$, we have $(xy)^2 = x^2y^2[x, y]$. But since $[P, P]$ has order 2, it is contained in $\mho^1(Z(P))$, and thus also $\varphi(\overline{xy}) = \varphi(\overline{x})\varphi(\overline{y})$. □

When $\Phi(P)$ has order p we have defined two maps on $P/\Phi(P)$. Note that in this situation $Z(P)$ has order at most p^2. The next lemma shows that the two maps φ and ψ coincide if and only if $Z(P)$ has order p. If $Z(P)$ has order p^2, then we obtain that φ is linear for p odd and quadratic for $p = 2$.

Lemma 1.3.17. *Suppose that $\Phi(P)$ has order p.*

a) If $Z(P)$ has order p, then $\varphi = \psi$.

b) If $Z(P)$ has order p^2, then $\varphi = 0$ and $\psi \neq 0$.

Proof. If $Z(P)$ has order p, then $\Phi(P) = Z(P) = Z(P)/\mho^1(Z(P))$ and the two maps are equal by definition. If $Z(P)$ has order p^2, then $\Phi(P) = \mho^1(Z(P))$, so that $\varphi = 0$. But if z is a generator of $Z(P)$, then z^p is a non-trivial element of $\Phi(P)$, so that $\psi(\overline{z}) \neq 0$. □

Classification of p-groups with a cyclic and central Frattini subgroup

We recall first the classification of p-groups with Frattini subgroup of order p. This can be found for example in [25] and we include the proof for the sake of completeness and to allow the reader to become familiar with the arguments.

Proposition 1.3.18. *Let p be an odd prime and let P be a non-abelian p-group with a Frattini subgroup of order p. Then $P/Z(P)$ has order $p^{2\ell}$, for some $\ell \geq 1$, and P is isomorphic to one of the following groups:*

1. $E \times X_{p^3}^{*\ell}$,
2. $E \times (X_{p^3}^{*(\ell-1)} * X_{p^3}^{-})$,
3. $E \times (X_{p^3}^{*\ell} * C_{p^2})$,

where E is elementary abelian of rank $\mathrm{rk}(Z(P)) - 1$.

Proof. Thanks to Lemma 1.3.2, we may suppose that $Z(P)$ is cyclic. Let z be a generator of $Z(P)$. Since $Z(P)$ is cyclic and all p-th powers are in $\Phi(P)$, we have that $Z(P)/\Phi(P)$ has order at most p. We let $w = z^p$ if $\Phi(P) < Z(P)$ and $w = z$ otherwise. In both cases w is a generator of $\Phi(P) = P'$ and this defines an isomorphism between $\Phi(P)$, resp. P', and the field $\mathbb{F}_p$.

Recall that the $\mathbb{F}_p$-vector space $V = P/\Phi(P)$ is endowed with the alternating form $b : V \times V \to P' \cong \mathbb{F}_p$ induced by commutators and $V^\perp = Z(P)/\Phi(P)$. Let $\psi : V \to \Phi(P) \cong \mathbb{F}_p$ be the linear map induced by taking p-th powers in P.

Suppose first that $Z(P) = \Phi(P)$, so that $V^\perp = 0$ and hence b is non-degenerate. In particular, $P/\Phi(P)$ has order $p^{2\ell}$ for some $\ell \geq 1$, and P has a symplectic set of generators $\{x_i, y_j \mid i = 1, \cdots, \ell\}$ satisfying

$$[x_i, y_i] = w, \text{ for all } 1 \leq i \leq \ell,$$
$$[x_i, x_j] = [x_i, y_j] = [y_i, y_j] = 1, \text{ for all } 1 \leq i \neq j \leq \ell.$$

If $\psi = 0$, the generators x_i, y_i all have order p and P is isomorphic to a central product $(X_{p^3})^{*\ell}$, that is P is extraspecial of type I.

If $\psi \neq 0$, then the symplectic generators can be chosen such that all but one, say y_ℓ, have order p and $y_\ell^p = w$ (see Proposition A.0.12). In this case, P is the central product of the subgroup generated by the elements x_i, y_i for $1 \le i \le \ell - 1$, which is isomorphic to $X_{p^3}^{*(\ell-1)}$, with the subgroup generated by x_ℓ and y_ℓ, which is isomorphic to $X_{p^3}^-$. Therefore P is extraspecial of type II in this case.

Suppose from now on that $\Phi(P) < Z(P)$, so that in particular $Z(P)$ is cyclic of order p^2. It follows that $V^\perp = Z(P)/\Phi(P)$ has dimension 1 over $\mathbb{F}_p$ and the class $\overline{z}$ of z modulo $\Phi(P)$ is a basis element of $V^\perp$. Note that by our choice of the generator of $\Phi(P)$, we have that $\psi(\overline{z}) = 1$.

Since ψ is a non-zero linear form, the subspace $W = \ker \psi$ has codimension 1 in V. Furthermore, the restriction of ψ to $V^\perp$ is not zero, since $\psi(\overline{z}) = 1$. It follows that W is a complement to $V^\perp$ in V, i.e. $V = W \oplus V^\perp$. The alternating form b is non-degenerate on W, so that we can then choose a symplectic basis $e_1, f_1, \cdots, e_\ell, f_\ell$ of W. Since $W = \ker \psi$ by definition, we have $\psi(e_i) = \psi(f_i) = 0$ for all $i = 1, \ldots, \ell$. We can take now representatives of the elements of the symplectic basis and we see that P is a central product of ℓ copies of X_{p^3} with a cyclic group of order p^2, namely $Z(P)$. □

Remark 1.3.19. It follows from Proposition 1.3.18 that a non-abelian p-group P with a Frattini subgroup of order p is uniquely defined by its order, its exponent, the order of $P/Z(P)$ and the order of $Z(P)$.

Proposition 1.3.20. *Let P be a non-abelian 2-group with a Frattini subgroup of order 2. Then $P/Z(P)$ has order $2^{2\ell}$, for some $\ell \ge 1$, and P is isomorphic to one of the following groups:*

1. $E \times D_8^{*\ell}$,
2. $E \times (D_8^{*(\ell-1)} * Q_8)$,
3. $E \times (D_8^{*\ell} * C_4)$,

where E is elementary abelian of rank $\mathrm{rk}(Z(P)) - 1$.

Proof. By Lemma 1.3.2, we may assume that P has a cyclic center. Recall that $V = P/\Phi(P)$ is endowed with a quadratic form $q : V \to \Phi(P)$ induced by the map sending any $x \in P$ to $x^2 \in \Phi(P)$. The polar form of q is the alternating form b induced by commutators. We mainly have to show that q is non-degenerate. The proposition will then follow directly from the classification of non-degenerate quadratic forms on $\mathbb{F}_2$-vector spaces (see Proposition A.0.20). Suppose thus that $x \in P$ is such that $[x, y] = 1 = x^2$, for all $y \in P$. This implies in particular that x is an element of order 2 of $Z(P)$. Hence $x \in \Phi(P)$ since $Z(P)$ is cyclic and the proposition is proved. □

Remark 1.3.21. In view of our convention that $D_8 = X_{2^3}$ and $Q_8 = X_{2^3}^-$, we could have given a single statement for p odd and $p = 2$. This statement would be exactly Proposition 1.3.18 but with the assumption that p is an arbitrary prime. Because of the difference in the proofs, the use of a linear form for p odd and a quadratic form for $p = 2$, we have preferred to give separate statements.

Proposition 1.3.18 and Proposition 1.3.20 give in particular a classification of the quasi-extraspecial p-groups having a Frattini subgroup of order p (this is the case $E = 1$ in the two above propositions). In order to obtain the classification of all quasi-extraspecial p-groups, it remains to consider the case when the Frattini subgroup has order at least p^2, and this is done in the following proposition. It has to be noted that now the proof works with absolutely no distinction between the two cases p odd and $p = 2$.

Proposition 1.3.22. *Let p be an arbitrary prime. Let P be a quasi-extraspecial p-group with $|\Phi(P)| = p^m$ and suppose $m > 1$. Then $P/Z(P)$ has order $p^{2\ell}$, for some $\ell \geq 1$, and $Z(P)$ has order p^r with $r \in \{m, m+1\}$. Moreover,*

1. *If $|Z(P)| = p^{m+1}$, then P is isomorphic to $X_{p^{2\ell+1}} * C_{p^{m+1}}$.*
2. *If $|Z(P)| = p^m$, then P is isomorphic to $X_{p^{2\ell-1}} * M_{p^{m+2}}$.*

Proof. Since P is quasi-extraspecial, it has a cyclic center which contains $\Phi(P)$. Let c be a generator of $Z(P)$. We must have $c^p \in \Phi(P)$, so that $\Phi(P)$ has index at most p in the cyclic group $Z(P)$. It follows that either $Z(P) = \Phi(P)$, in which case $Z(P)$ has order p^m, or $\Phi(P)$ is maximal in $Z(P)$, in which case $Z(P)$ has order p^{m+1}. This proves our assertion on the order of $Z(P)$.

Let $z = c^{p^{r-1}}$ be a generator of the unique subgroup of order p in $Z(P)$. Since $\Phi(P)$ is central, we have from Lemma 1.3.3 that P' has order p and hence $P' = \langle z \rangle$.

Let $V = P/Z(P)$. Recall that taking p-th powers of elements of P induces a linear form $\varphi : V \to Z(P)/\mho^1(Z(P))$. Furthermore, this linear form is zero if $\Phi(P)$ is strictly contained in $Z(P)$, i.e. if $Z(P)$ has order p^{m+1}, and is non-zero if $\Phi(P) = Z(P)$, i.e. $Z(P)$ has order p^m. Recall also that V is a non-degenerate alternating space with respect to the form $b : V \times V \to \mathbb{F}_p \cong \langle z \rangle$ induced by commutators. As a first consequence, V has even dimension over $\mathbb{F}_p$, say 2ℓ for some $\ell \geq 1$. It follows, in particular, that $V = P/Z(P)$ has order $p^{2\ell}$ and this proves our assertion on the order of $P/Z(P)$.

The vector space $V = P/Z(P)$ admits a symplectic basis $e_1, f_1, \ldots, e_\ell, f_\ell$ such that $\varphi(e_i) = \varphi(f_i) = \varphi(e_\ell) = 0$, for $i = 1, \ldots, \ell-1$, and $\varphi(f_\ell) = 1$ if $\varphi \neq 0$. Let $x_1, y_1, \ldots, x_\ell, y_\ell$ be representatives in P of the elements of this symplectic basis. These elements together with the generator of $Z(P)$ generate the group P and satisfy the following conditions:

$$[x_i, x_j] = [x_i, y_j] = [y_i, y_j] = 1, \text{ for all } 1 \leq i \neq j, \leq \ell. \tag{1.11}$$

$$[x_i, y_i] = z, \text{ for all } i = 1, \ldots, \ell. \tag{1.12}$$

Assertion 1. *If $\varphi = 0$, the representatives $x_1, y_1, \ldots, x_\ell, y_\ell$ can be chosen such that they satisfy the following additional condition:*

$$x_i^p = y_i^p = 1, \text{ for all } i = 1, \ldots, \ell. \tag{1.13}$$

The condition $\varphi(e_i) = 0$ implies that x_i^p is in $\mho^1(Z(P)) =< c^p >$, so that $x_i^p = (c^p)^{k_i}$. In particular, $(x_i c^{-k_i})^p = 1$. For $i = 1, \ldots, \ell$, let $x_i' = x_i c^{-k_i}$, so that $x_i' \in x_i Z(P)$ and $(x_i')^p = 1$. With the same argument, we can find $y_i' \in y_i Z(P)$, with $(y_i')^p = 1$. The elements $x_1', y_1', \ldots, x_\ell', y_\ell'$ satisfy the required condition and still satisfy conditions (1.11) and (1.12) above. This proves Assertion 1.

Assertion 2. *If $\varphi \neq 0$, the representatives $x_1, y_1, \ldots, x_\ell, y_\ell$ can be chosen such that the satisfy the following two additional conditions:*

$$x_i^p = y_i^p = 1, \text{ for all } i = 1, \ldots, \ell - 1. \tag{1.14}$$

$$x_\ell^p = 1 \text{ and } y_\ell^{p^m} = [x_\ell, y_\ell]. \tag{1.15}$$

If φ is non-zero, the symplectic basis $e_1, f_1, \ldots, e_\ell, f_\ell$ can be chosen such that $\varphi(e_i) = \varphi(f_i) = \varphi(e_\ell) = 0$ for $i = 1, \ldots, \ell - 1$, and $\varphi(f_\ell) = 1$. With an argument similar to the one used in the proof of the previous assertion, we may suppose that $x_i^p = y_i^p = x_\ell^p = 1$ for $i = 1, \ldots, \ell - 1$. The condition $\varphi(f_\ell) = 1$ implies that $(y_\ell)^p = c^{1+pk}$, for some k and in particular, $y_\ell^{p^m} = z = [x_\ell, y_\ell]$. This proves Assertion 2.

If $\varphi = 0$, the three conditions (1.11), (1.12) and (1.13) show that the subgroup X generated by $x_1, y_1, \ldots, x_\ell, y_\ell$ is extraspecial of type I. In this case, $P = XZ(P)$ and $X \cap Z(P) = Z(X)$, so that $P = X * Z(P)$ and hence P is isomorphic to $X^+_{p^{2l+1}} * C_{p^{m+1}}$.

If $\varphi \neq 0$, the conditions (1.11) and (1.12) together with the conditions (1.14) and (1.15) show that P is a central product of the subgroup generated by $x_1, y_1, \ldots, x_{\ell-1}, y_{\ell-1}$, which is extraspecial of type I, and the subgroup generated by x_ℓ, y_ℓ, which is isomorphic to $M_{p^{m+2}}$. We obtain thus that P is a central product $X_{p^{2\ell-1}} * M_{p^{m+2}}$. □

Remark 1.3.23. This classification, with a similar approach, already appears in a paper by Newman [21]. The main difference is that Newmann does not consider p-th powers as a linear form. As can be seen in [21], the linear form is not of particular importance for this classification. It brings at most more conceptuality and clarify some of the arguments. The usefulness of the linear form will however become more evident in the determination of automorphism groups of quasi-extraspecial p-groups performed in Chapter 3.

It can be deduced from Proposition 1.3.22 that quasi-extraspecial p-groups with a Frattini subgroup of order at least p^2 are determined, up to isomorphism, by their order, the order of the Frattini subgroup and the rank of the central quotient. This is the content of the following corollary.

Corollary 1.3.24. *Let $\ell \geq 1$ and $m > 1$. Up to isomorphism, there exists a unique quasi-extraspecial p-group P of a given order and such that $\Phi(P) = p^m$ and $P/Z(P)$ has rank 2ℓ.*

Remark 1.3.25. The previous corollary is not true for $m = 1$, since the groups $X^-_{p^3}$ and X_{p^3} are not isomorphic.

Recall from Lemma 1.3.2 that p-groups with cyclic and central Frattini subgroup are obtained as direct products of a quasi-extraspecial p-group with an elementary abelian p-group. This, together with the above propositions, shows the following general theorem classifying all p-groups with a cyclic and central Frattini subgroup.

Theorem 1.3.26. *Let p be a prime and let P be a non-abelian p-group with a cyclic and central Frattini subgroup. Let $|\Phi(P)| = p^m$, then $|P/Z(P)| = p^{2\ell}$, for some $\ell \geq 1$, and P is isomorphic to a direct product $E \times Q$, where E is elementary abelian of rank* $\mathrm{rk}(Z(P)) - 1$ *and Q satisfies the following:*

a) If p is odd, then Q is isomorphic to one of the following groups:

(i) $X_{p^3}^{*\ell}$;

(ii) $X_{p^3}^{*(\ell-1)} * X_{p^3}^{-}$;

(iii) $X_{p^3}^{*\ell} * C_{p^{m+1}}$, *with* $m \geq 1$;

(iv) $X_{p^3}^{*(\ell-1)} * M_{p^{m+2}}$, *with* $m > 1$.

b) If $p = 2$, then Q is isomorphic to one of the following groups:

(i) $D_8^{*\ell}$;

(ii) $D_8^{*(\ell-1)} * Q_8$;

(iii) $D_8^{*\ell} * C_{2^{m+1}}$, *with* $m \geq 1$;

(iv) $D_8^{*(\ell-1)} * M_{2^{m+2}}$, *with* $m > 1$.

Remark 1.3.27.

a) This classification can be deduced from the more general classification of p-groups with cyclic Frattini subgroup performed by Berger, Kovács and Newman in [4]. The part of their proof that we are concerned with here, namely the case of a central and cyclic Frattini subgroup, is however left to the reader in [4].

b) As noted in [4], when p is odd, the condition $Z(\Phi(P))$ cyclic implies that $\Phi(P)$ is cyclic. This result is originally due to Hobby [17] (see also (4.2) in Suzuki [27]). The classification above is then a classification of all odd order p-groups such that $Z(\Phi(P))$ is cyclic.

Classification of 2-groups with a non-central cyclic Frattini subgroup

Contrary to the case p odd, there exist 2-groups with a non-central cyclic Frattini subgroup. Classical examples are the dihedral groups $D_{2^{m+2}}$, the semi-dihedral groups $SD_{2^{m+2}}$ and the quaternion groups $Q_{2^{m+2}}$, all for $m > 1$. Two more examples are the groups $D_{2^{m+3}}^{+}$ and $Q_{2^{m+3}}^{+}$ that will be defined below (see also [4] for the original definitions and notation).

Recall that for $m > 1$, the automorphism group of $C_{2^{m+1}}$ contains a unique elementary abelian subgroup of rank 2.

Definition 1.3.28. For $m > 1$, the group $D_{2^{m+3}}^{+}$ is defined as the semi-direct product $C_{2^{m+1}} \rtimes (C_2 \times C_2)$ with respect to the action given by the canonical inclusion $C_2 \times C_2 \hookrightarrow \mathrm{Aut}(C_{2^{m+1}})$.

The group $D^+_{2^{m+3}}$ has the following presentation:

$$D^+_{2^{m+3}} = \langle a, b, u \mid a^2 = b^2 = u^{2^{m+1}} = 1, [a, b] = 1, [a, u] = u^{2^m}, [b, u] = u^{-2} \rangle. \tag{1.16}$$

Lemma 1.3.29. *Let $m > 1$ and let b, u be generators of the group $Q_{2^{m+2}}$ with b of order 4, u of order 2^{m+1} and such that $bub^{-1} = u^{-1}$. The homomorphism α induced by $u \mapsto u^{1+2^m}$ and $b \mapsto b$ is an automorphism of $Q_{2^{m+2}}$ of order 2.*

Proof. It is not difficult to see that α preserves the order of the generators and the relations between them. It can be thus extended to an automorphism of $Q_{2^{m+2}}$. It is then easy to check that α^2 is the identity. $\square$

Definition 1.3.30. For $m > 1$, the group $Q^+_{2^{m+3}}$ is defined as the semi-direct product $Q_{2^{m+2}} \rtimes C_2$ with respect to the action given by the automorphism α of Lemma 1.3.29.

The group $Q^+_{2^{m+3}}$ has the following presentation:

$$Q^+_{2^{m+3}} = \langle a, b, u \mid a^2 = u^{2^{m+1}} = 1, b^2 = u^{2^m}, [a, b] = 1, [a, u] = u^{2^m}, [b, u] = u^{-2} \rangle. \tag{1.17}$$

Let us make some small remarks on the structure of these groups.

Remark 1.3.31.

a) In the two presentations above, the commutator relations can be written as $aua^{-1} = u^{1+2^m}$ and $bub^{-1} = u^{-1}$. It follows also that ab acts on u as $(ab)u(ab)^{-1} = u^{-1+2^m}$. These are the three possible actions of order 2 on the generator of a cyclic group of order 2^{m+1}.

b) As for $D^+_{2^{m+3}}$, the group $Q^+_{2^{m+3}}$ is an extension of $C_2 \times C_2$ by C_{2^m} under the faithful action, but in this case the extension does not split.

c) The quotient $D^+_{2^{m+3}}/\langle u \rangle$ is elementary abelian of rank 2. The group $D^+_{2^{m+3}}$ has thus three maximal subgroups. The maximal subgroup $\langle a, u \rangle$ is isomorphic to $M_{2^{m+2}}$, the subgroup $\langle ab, u \rangle$ is isomorphic to $SD_{2^{m+2}}$ and the subgroup $\langle b, u \rangle$ is isomorphic to $D_{2^{m+2}}$. Their intersection is the cyclic subgroup $\langle u \rangle$ of order 2^{m+1}. These subgroups are visually depicted in Figure 1.1.

d) The group $Q^+_{2^{m+3}}$ has three maximal subgroups, namely $\langle a, u \rangle = M_{2^{m+2}}$, $\langle ab, u \rangle = SD_{2^{m+2}}$ and $\langle b, u \rangle = Q_{2^{m+2}}$. These subgroups are visually depicted in Figure 1.2.

e) The element ab has order 2 in $D^+_{2^{m+3}}$. It follows that the non-central elements of order 2 in the maximal subgroup $\langle ab, u \rangle = SD_{2^{m+2}}$ are those of the form abu^k with k even. The elements of the form abu^j with j odd have order 4. In the case of the group $Q^+_{2^{m+3}}$ the element ab has order 4, so that the elements abu^i have order 2 if i is odd and order 4 if i is even. It may be useful to keep this difference in mind when working with the elements of these groups.

f) In what follows, these groups will appear as an extension of the maximal subgroup $M_{2^{m+2}}$.

$$\begin{tikzcd}
& D^+_{2^{m+3}} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
D_{2^{m+2}} \arrow[dr, dash] & M_{2^{m+2}} \arrow[d, dash] & SD_{2^{m+2}} \arrow[dl, dash] \\
& C_{2^{m+1}} &
\end{tikzcd}$$

Figure 1.1: Maximal subgroups of $D^+_{2^{m+3}}$

$$\begin{tikzcd}
& Q^+_{2^{m+3}} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
Q_{2^{m+2}} \arrow[dr, dash] & M_{2^{m+2}} \arrow[d, dash] & SD_{2^{m+2}} \arrow[dl, dash] \\
& C_{2^{m+1}} &
\end{tikzcd}$$

Figure 1.2: Maximal subgroups of $Q^+_{2^{m+3}}$

Of course, these two groups satisfy the desired conditions on the Frattini subgroup.

Lemma 1.3.32. *Let P be the group $D^+_{2^{m+3}}$ or $Q^+_{2^{m+3}}$ for some $m > 1$. Then P has order 2^{m+3} and $\Phi(P)$ is cyclic of order 2^m, but is not central in P.*

Proof. This is clear from the above presentations that $\Phi(P)$ is generated by u^2, so is cyclic of order 2^m. But the generator b acts non-trivially on u^2 since $bu^2b^{-1} = u^{-2}$ and $m > 1$. $\square$

Let P be a 2-group with a non-central cyclic Frattini subgroup. The determination of the structure of P goes as follows. First, we will show that the centralizer C_0 of $\Phi(P)$ in P is maximal in P. Since $\Phi(P)$ is obviously central in its centralizer, we obtain that C_0 is a 2-group with a cyclic and central Frattini subgroup. The group P has thus a maximal subgroup C_0 that can be described reasonably well thanks to the classification obtained previously. It remains then to describe how an element outside of C_0 acts on C_0.

Lemma 1.3.33. *If P is a 2-group with $\Phi(P)$ cyclic, there exists $u \in P$ such that $\Phi(P) = \langle u^2 \rangle$.*

Proof. Since $P/\mho^1(P)$ has exponent 2, hence is also abelian, we have that $\Phi(P) \leq \mho^1(P)$. The reverse inclusion holds trivially, so that $\Phi(P) = \mho^1(P)$ is cyclic. The lemma follows now from Lemma 1.3.4. $\square$

Lemma 1.3.34. *If P is a 2-group with $\Phi(P)$ cyclic, then $|P : C_P(\Phi(P))| \leq 2$.*

Proof. It is clear if $\Phi(P)$ is central in P, so suppose that $C_P(\Phi(P))$ is strictly contained in P. In particular, if $|\Phi(P)| = 2^m$, then $m > 1$.

Let $u \in P$ such that $\Phi(P) = \langle u^2 \rangle$, the subgroup $U = \langle u \rangle$ is cyclic of order 2^{m+1} and contains $\Phi(P)$, hence is normal in P. Furthermore, we have the following inclusions of subgroups of P:

$$\Phi(P) \leq U \leq C_P(U) \leq C_P(\Phi(P)) < P.$$

In particular, $P/C_P(U)$ is an elementary abelian 2-group and the action of P on U by conjugation induces an injective homomorphism $P/C_P(U) \to \mathrm{Aut}(U)$. The characterization of the automorphism group of a cyclic 2-group implies that $|P/C_P(U)| \leq 4$.

If $|P/C_P(U)| = 4$, there must exist $x \in P$ such that $xux^{-1} = u^{1+2^m}$. But then, $xu^2x^{-1} = u^2$, hence $x \in C_P(\Phi(P))$. But $x \notin C_P(U)$, so that the following inclusions are strict:

$$C_P(U) < C_P(\Phi(P)) < P.$$

Since $|P : C_P(U)| = 4$, we must have $|P : C_P(\Phi(P))| = 2$. If $|P : C_P(U)| = 2$, the same conclusion holds trivially and the lemma is proved. $\square$

Lemma 1.3.35. *Let P be a 2-group with a non-central cyclic Frattini subgroup. Let $C_0 = C_P(\Phi(P))$, then $\Phi(C_0) = \Phi(P)$ and $\Phi(C_0)$ is central in C_0.*

Proof. Let $U = \langle u \rangle$, where $u \in P$ is such that $\Phi(P) = \langle u^2 \rangle$. Since $U \leq C_0$, we have $u^2 \in \Phi(C_0)$, and thus $\Phi(P) \leq \Phi(C_0)$. The inclusion $\Phi(C_0) \leq \Phi(P)$ is trivially true, so that $\Phi(C_0) = \Phi(P)$. It is then clear that $\Phi(C_0)$ is central in C_0. $\square$

Proposition 1.3.36. *Let P be a 2-group with $\Phi(P)$ cyclic of order 2^m and not central in P. Let $Z = \Omega_1(\Phi(P))$, there exists two subgroups Q and S of P such that*

a) $P = Q \underset{Z}{*} S$,

b) $\Phi(Q) = Z$ *is cyclic of order 2,*

c) S *is either dihedral, semi-dihedral or quaternion and of order* 2^{m+2}*, or isomorphic to* $D^+_{2^{m+3}}$ *or* $Q^+_{2^{m+3}}$.

Proof. By the classification of 2-groups with a cyclic and central Frattini subgroup, the subgroup $C_0 = C_P(\Phi(P))$ can be written as $E \times (D * M)$, with E elementary abelian, D isomorphic to $D_8^{*\ell}$ and M is either cyclic of order 2^{m+1}, or isomorphic to $M_{2^{m+2}}$.

We choose $b \notin C_0$ and let S be the subgroup generated by M and b. As a first step, we will describe the possible structure of this subgroup S. Recall from Lemma 1.3.35 that $\Phi(P) = \Phi(C_0)$. It follows in particular that $\Phi(P)$ is contained in M. As a consequence, we have that M is normal in P, hence in S. Furthermore M has index 2 in S, since $b^2 \in \Phi(P) \leq M$.

If M is cyclic, then S has a maximal cyclic subgroup. Furthermore $\Phi(P)$ is not central in S by the choice of b. This, together with Lemma 1.2.9 classifying

p-groups with a maximal cyclic subgroup, shows that S is either dihedral, semi-dihedral or quaternion.

Suppose now that M is isomorphic to $M_{2^{m+2}}$ and let u, a be generators of M such that a has order 2, u has order 2^{m+1} and $aua^{-1} = u^{1+2^m}$. The subgroup S is generated by a, u and the element $b \notin C_0$. Furthermore, the subgroup generated by u is normal in P, since it contains $\Phi(P) = \langle u^2 \rangle$.

The element b does not centralize $\Phi(P) = \langle u^2 \rangle$ and acts on the cyclic 2-group $U = \langle u \rangle$ as an automorphism of order 2, since $b^2 \in \Phi(P) \leq U$. It follows that b acts on u either by $bub^{-1} = u^{-1}$, or by $bub^{-1} = u^{-1+2^m}$. If $bub^{-1} = u^{-1+2^m}$, we replace b by ba, so that we may assume that $bub^{-1} = u^{-1}$.

Remark that on the one hand, we have $b^2 \in \Phi(P)$ on which b acts by taking the inverse and on the other hand, b acts trivially on b^2. It follows that b^2 has order at most 2, hence b has order 2 or 4.

We have already seen that $M = \langle u, a \rangle$ is a normal subgroup of P. We consider now the action of b on M. Let $z = u^{2^m}$, the subgroup $\Omega_1(M) = \langle z, a \rangle$ is characteristic in M, hence normal in P. The same holds for $\Omega_1(Z(M)) = \langle z \rangle$. Therefore, we have either that b acts trivially on a, or that $bab^{-1} = za$. If $bab^{-1} = za = u^{2^m}a$, we replace b by bu^{-1}, in order to have that b and a commute. Remark that this does not change the action of b on u, nor the order of b. We have thus that the subgroup S is generated by a, b and u, with u of order 2^{m+1}, a of order 2, $aua^{-1} = u^{1+2^m}$, $bub^{-1} = u^{-1}$, $[a, b] = 1$ and b has order at most 4. This shows that S is isomorphic to $D^+_{2^{m+3}}$ or $Q^+_{2^{m+3}}$, depending on the order of b.

To summarize, we have thus showed that S is either dihedral, semi-dihedral, quaternion and of order 2^{m+2} (case M cyclic), or isomorphic to $D^+_{2^{m+3}}$ or $Q^+_{2^{m+3}}$ (case M isomorphic to $M_{2^{m+2}}$). The next step is to decompose P as a central product $P = Q * S$.

The group P is generated by the subgroup $E \times D$ and the subgroup S. Furthermore, $S \cap C_0 = M$, so that $(E \times D) \cap S = (E \times D) \cap M = \langle z \rangle$ is cyclic of order 2. However, these two subgroups $E \times D$ and S may not commute, since $\langle b \rangle$ does not necessarily commute with $(E \times D)$. Note however that $E \times D$ commutes with the subgroup M, by the choice of the decomposition of C_0. We show now how the subgroups E and D have to be modified so that they commute with S.

Let $e_1, \ldots, e_t$ be linearly independent generators of the elementary abelian group E. Let H be the subgroup generated by $\Phi(P)$ and b. The subgroup H is normal in P, since H contains $\Phi(P)$, and the subgroup E acts on H as automorphisms of order 1 or 2 fixing $\Phi(P)$. For any $i = 1, \ldots, t$, we have thus that either e_i and b commute, or $e_i b e_i^{-1} = u^{2^m} = zb$. Let $w = u^{2^{m-1}}$ be one of the elements of order 4 in $\langle u \rangle$. Since $bub^{-1} = u^{-1}$, we have $wbw^{-1} = bz$. For $i = 1, \ldots, t$, let

$$f_i = \begin{cases} e_i & \text{if } [e_i, b] = 1. \\ e_i w & \text{otherwise .} \end{cases}$$

Remark that now $f_i b f_i^{-1} = b$, for all $i = 1, \ldots, t$. Since w is centralized by E, we have $[e_i, e_j] = [f_i, f_j] = 1$ for $1 \leq i, j \leq t$. Since $w^2 = z$, we have either $f_i^2 = 1$ or $f_i^2 = z$, for $i = 1, \ldots, t$. It follows that the subgroup E_0 generated by these elements f_i, $i = 1, \ldots, t$, is abelian with $\Phi(E_0) \leq \langle z \rangle$. Since w is central in M and is centralized by E_0, we have that E_0 commutes with S.

Let $x_1, y_1, \ldots, x_\ell, y_\ell$ be symplectic generators of the subgroup D such that

$[x_i, y_i] = z$. With an argument similar to the one performed for the subgroup E, we can modify the generators of D by the element w, if needed, in such a way that D commutes with $\langle b \rangle$ and hence with S. We denote D_0 the subgroup obtained from D after eventual modification of the generators x_i, y_i, $i = 1, \dots, \ell$. Since w is centralized by D, we have $\Phi(D_0) = \langle z \rangle$ and by construction D_0 commutes with S.

Denote by Q the subgroup generated by E_0 and D_0. Since E_0 and D_0 commute with S, we have that P is a central product $P = Q * S$. Since E_0 and D_0 commute and $\Phi(E_0) = \Phi(D_0) = \langle z \rangle$, we have also that $\Phi(Q) = \langle z \rangle$ and the proposition is proved. □

We can now state and prove our second main result towards the classification of p-groups with a cyclic Frattini subgroup. The original result, with a different approach, is due to Berger, Kovács and Newman [4].

Theorem 1.3.37. *Let P be a 2-group with a cyclic and non-central Frattini subgroup and let $2^m = |\Phi(P)|$. Then $m > 1$ and P is isomorphic to a product $E \times (D_8^{*\ell} * H)$, where E is elementary abelian, $\ell \geq 0$ and H is a non-trivial group isomorphic to one of the following groups:*

$$D_{2^{m+2}}, Q_{2^{m+2}}, SD_{2^{m+2}}, D_{2^{m+2}} * C_4, SD_{2^{m+2}} * C_4, D^+_{2^{m+3}}, Q^+_{2^{m+3}} or D^+_{2^{m+3}} * C_4. \tag{1.18}$$

Proof. Since $\Phi(P)$ is normal in P, we have $\Phi(P) \cap Z(P) \neq 1$. Since $\Phi(P)$ is not central by assumption, we have $|\Phi(P)| > 2$ and hence $m > 1$.

Let $Z = \Omega_1(\Phi(P))$. By the preceding proposition, we know that P is a central product $Q \underset{Z}{*} S$, with $|\Phi(Q)| = 2$. It follows from Proposition 1.3.20 that Q is isomorphic to one of the following groups:

$$E \times D_8^{*\ell},$$
$$E \times (D_8^{*\ell} * C_4),$$
$$E \times (D_8^{*\ell-1} * Q_8),$$

where E is elementary abelian. The group S is either dihedral, semi-dihedral, quaternion and of order 2^{m+2}, or isomorphic to $D^+_{2^{m+3}}$ or $Q^+_{2^{m+3}}$. These five cases will be denoted by $\mathbf{d}, \mathbf{s}, \mathbf{q}, \mathbf{d}^+$ and $\mathbf{q}^+$ respectively.

We have thus that P is a central product $P = E \times (D_8^{*\ell} * R * S)$, where R is either D_8, C_4, or Q_8. These three cases will be denoted respectively by $\mathbf{D}$, $\mathbf{C}$, and $\mathbf{Q}$. We write T for the subgroup $R * S$ and we will write $T = \mathbf{D} * \mathbf{d}$ if $R = D_8$ and $S = D_{2^{m+2}}$. The other cases are written similarly. We have thus that $P = E \times (D_8^{*\ell-1} * T)$, and it remains to identify all the possible choices for T. For this, it is enough to see when two different central product $R * S$ are isomorphic, when R and S are chosen in their respective list.

For example, the case $T = \mathbf{D} * \mathbf{d}$ is isomorphic to the case $T = \mathbf{Q} * \mathbf{d}$, since $Q_8 * D_{2^{m+2}} \cong D_8 * D_{2^{m+2}}$. In this case, we obtain $P = E \times (D_8^{*\ell} * D_{2^{m+2}})$. The theorem follows now from the following identifications.

- $\mathbf{D} * \mathbf{d}$ is isomorphic to $\mathbf{Q} * \mathbf{d}$, since $D_8 * D_{2^{m+2}} \cong Q_8 * D_{2^{m+2}}$. In this case, $P = E \times (D_8^{*\ell} * D_{2^{m+2}})$.

- $\mathbf{D} * \mathbf{q}$ is isomorphic to $\mathbf{Q} * \mathbf{q}$, since $D_8 * Q_{2^{m+2}} \cong Q_8 * Q_{2^{m+2}}$. In this case, $P = E \times (D_8^{*\ell} * Q_{2^{m+2}})$.
- $\mathbf{D} * \mathbf{s}$ is isomorphic to $\mathbf{Q} * \mathbf{s}$, since $D_8 * SD_{2^{m+2}} \cong Q_8 * SD_{2^{m+2}}$. In this case, $P = E \times (D_8^{*\ell} * SD_{2^{m+2}})$.
- $\mathbf{C} * \mathbf{d}$ is isomorphic to $\mathbf{C} * \mathbf{q}$, since $Q_{2^{m+2}} * C_4 \cong D_{2^{m+2}} * C_4$. In this case, $P = E \times (D_8^{*\ell} * D_{2^{m+2}} * C_4)$.
- In the case $\mathbf{C} * \mathbf{s}$, then $P = E \times (D_8^{*\ell} * SD_{2^{m+2}} * C_4)$.
- $\mathbf{D} * \mathbf{d}^+$ is isomorphic to $\mathbf{Q} * \mathbf{q}^+$, since $D_8 * D^+_{2^{m+3}} \cong Q_8 * Q^+_{2^{m+3}}$. In this case, $P = E \times (D_8^{*\ell} * D^+_{2^{m+3}})$.
- $\mathbf{D} * \mathbf{q}^+$ is isomorphic to $\mathbf{Q} * \mathbf{d}^+$, since $D_8 * Q^+_{2^{m+3}} \cong Q_8 * D^+_{2^{m+3}}$. In this case, $P = E \times (D_8^{*\ell} * Q^+_{2^{m+3}})$.
- $\mathbf{C} * \mathbf{d}^+$ is isomorphic to $\mathbf{C} * \mathbf{q}^+$, since $C_4 * D^+_{2^{m+3}} \cong C_4 * Q^+_{2^{m+3}}$. In this case, $P = E \times (D_8^{*\ell} * D^+_{2^{m+3}} * C_4)$.

□

Remark 1.3.38. If P is a 2-group with a cyclic and non-central Frattini subgroup, then Theorem 1.3.37 says that $P = E \times (D_8^{*\ell} * H)$, with E elementary abelian, $\ell \geq 0$ and H is one of the groups in the list (1.18). It is not difficult to see that two groups in the list (1.18) are never isomorphic and that, up to isomorphism, P is determined by the rank of E, the integer ℓ and the subgroup H.

1.4 Classification of odd order p-groups of class 2 with a cyclic center

Throughout this section, p always denotes an odd prime number. Note that we will however make additional remarks for the case $p = 2$ at the end of this section.

In this section, we give results towards the classification of p-groups of class 2 with a cyclic center. A decomposition of these groups as central products of 2-generator groups was given by other means by Brady, Bryce and Cossey [9]. The isomorphism problem for these groups was solved by Leong in [19] for p odd, and in [20] for $p = 2$. When p is odd, we will recover their results by expanding the method used in Section 1.3.

If P is a p-group of class 2 with a cyclic center, then in particular P' is cyclic, say of order p^m, and the choice of a generator gives an isomorphism between P' and the ring $R = \mathbb{Z}/p^m\mathbb{Z}$. If V denotes the quotient group $P/Z(P)$, the commutators induce a map

$$b : V \times V \to R,$$

and this map satisfies conditions of bilinearity (1.3) and (1.4), alternation (1.1) and regularity (1.2). To begin, we will consider the case where V is a free R-module, that is the abelian group $P/Z(P)$ is homocyclic of type p^m. In this situation, there exists a symplectic basis on V and we will see furthermore that taking p^m-th powers in P induces a linear form on V. The classification of these groups will follow from general results on alternating free modules over $\mathbb{Z}/p^m\mathbb{Z}$. These results are very similar to the usual results for vector spaces and the reader is referred to Appendix A for the details.

In a second part, we will see that any p-group of class 2 with a cyclic center can be decomposed as a central product $P = Z(P) * Q_1 * \cdots * Q_t$, where, for each k, Q_k is a p-group of class 2 with a cyclic center and such that the quotient $Q_k/Z(Q_k)$ is homocylic of type p^{m_k}, for some $m_k \geq 1$. By the first part, the structure of these groups Q_k is known and this gives a decomposition of P. We will see how a canonical decomposition can be deduced from this one.

The homocyclic case

Recall that p is an odd prime number. We fix a p-group P of class 2 with a cyclic center and such that the quotient group $P/Z(P)$ is homocyclic of type p^m. Remark that for $m = 1$, the p-group P has a cyclic center and a central Frattini subgroup, hence is quasi-extraspecial in our terminology. The methods used in Section 1.3 generalize rather easily for $m > 1$. The following two results correspond respectively to Lemma 1.3.3 and Lemma 1.2.2 when specialized to $m = 1$.

Lemma 1.4.1. *The central quotient $P/Z(P)$ has exponent p^m if and only if P' has order p^m.*

Proof. Let p^a denote the exponent of $P/Z(P)$ and let $p^m = |P'|$. We have to show that $a = m$. Since $P' \leq Z(P)$, we have $[x, y]^k = [x^k, y]$, for all $k \in \mathbb{Z}$ and $x, y \in P$. In particular, $[x, y]^{p^a} = [x^{p^a}, y] = 1$, since $x^{p^a} \in Z(P)$, so that $m \leq a$.

Let $x \in P$ such that $xZ(P)$ has order p^a in $P/Z(P)$. We have $1 = [x, y]^{p^m} = [x^{p^m}, y]$, for all $y \in P$, so that $x^{p^m} \in Z(P)$ and hence $m \geq a$. □

Lemma 1.4.2. *For all $x, y \in P$, we have*

$$(xy)^{p^m} = x^{p^m} y^{p^m}.$$

Proof. Since $P' \leq Z(P)$, we have

$$(xy)^{p^m} = [y, x]^{\frac{p^m(p^m-1)}{2}} x^{p^m} y^{p^m}.$$

Since p is odd and P' has order p^m, then $[y, x]^{\frac{p^m(p^m-1)}{2}} = 1$. □

We give now two examples of p-groups of class 2 with a homocyclic quotient group $P/Z(P)$. These groups will be building blocks for all p-groups with this property. The first example is a generalization of extraspecial p-groups of type I.

Definition 1.4.3. For $\ell \geq 1$ and $m \geq 1$, we define $X_{2\ell+1}(p^m)$ as the subgroup of $U_{\ell+2}(\mathbb{Z}/p^m\mathbb{Z})$ given by matrices of the form

$$\begin{pmatrix} 1 & * & \cdots & * \\ & \ddots & 0 & \vdots \\ & 0 & \ddots & * \\ & & & 1 \end{pmatrix}.$$

When $\ell = 1$, the group $X_3(p^m)$ has the following presentation

$$X_3(p^m) = \langle x, y \,|\, x^{p^m} = y^{p^m} = 1, [x,y]^{p^m} = 1, [x,[x,y]] = [y,[x,y]] = 1\rangle$$

Remark 1.4.4. When $m = 1$, $X_{2\ell+1}(p)$ is the extraspecial group of type I and order $p^{2\ell+1}$. This motivates our notation, since then $X_{p^{2\ell+1}} = X_{2\ell+1}(p)$.

The next lemma shows that these groups $X_3(p^m)$ have (at least) the desired properties, namely, they have a cyclic center and the quotient by the center is a homocyclic abelian group.

Lemma 1.4.5. *If $P = X_{2\ell+1}(p^m)$, then*

a) $Z(P) = P'$ and is cyclic of order p^m,

b) $\mho^m(P) = \{1\}$,

c) $P/Z(P)$ is isomorphic to a direct product $(C_{p^m})^{2\ell}$,

d) P has order $p^{m(2\ell+1)}$,

e) P is isomorphic to a central product of ℓ copies of $X_3(p^m)$.

Proof. Let $e_{i,j}$ be the elementary matrix with 1 in the (i,j)-th entry and 0 elsewhere. We remark that for $i \neq j$, we have $(I + e_{i,j})^m = I + me_{i,j}$, so that the group P is generated by all the matrices $I + e_{1,j}$ and $I + e_{k,\ell+2}$, with $1 < j \leq \ell+2$ and $1 \leq k < \ell+2$. For $1 < j,k < \ell+2$, an elementary calculation shows that

$$[I + e_{1,j}, I + e_{k,\ell+2}] = I + \delta_{j,k}e_{1,\ell+2}. \tag{1.19}$$

Similarly,

$$[I + e_{1,j}, I + e_{1,\ell+2}] = [I + e_{\ell+2,k}, I + e_{1,\ell+2}] = 0, \text{ for } 1 < j,k < \ell+2. \tag{1.20}$$

It follows that $I + e_{1,\ell+2}$ is central and all commutators between the generators of P are central. As a consequence, $Z(P) = P' = \langle I + e_{1,\ell+2}\rangle$. It follows from Lemma 1.4.2 that $\mho^m(P) = 1$ and using Lemma 1.4.1, we see that $P/Z(P)$ is homocyclic of type p^m.

For $1 < j < \ell+2$ the subgroup H_j generated by $I + e_{1,j}$ and $I + e_{j,\ell+2}$ is isomorphic to $X_3(p^m)$ with $Z(H_j) = Z(P)$. It follows from (1.19) and (1.20), that P decomposes as a central product $P = H_1 * \cdots * H_\ell$. □

Remark 1.4.6. The amalgamation in $X_3(p^m)^{*\ell}$ is made along the center of the groups $X_3(p^m)$. Let us see briefly that this amalgamation is independent of the chosen isomorphism. If P is the group $X_3(p^m)$, then any automorphism of $Z(P)$ sends the generator z of $Z(P)$ to z^k for some k prime to p. Similarly to what we made for extraspecial p-groups, we can extend this automorphism to the whole group P by defining $x \mapsto x^k$ and $y \mapsto y$.

As a second example, we will define generalizations of the groups $M_{p^{m+2}}$. We will define these groups as semi-direct products and for this, we will need the automorphism given by the following lemma.

Lemma 1.4.7. *Let $m \geq 1$ and $s \geq 0$ be such that $m \geq s$, and let P be the central product $C_{p^{m+s}} \underset{C_{p^s}}{*} C_{p^m}$. Denote by y, respectively z, a generator of $C_{p^{m+s}}$, respectively C_{p^m}. The map $\alpha : P \to P$ defined by $\alpha(z) = z$ and $\alpha(y) = yz$ is an automorphism of P of order p^m.*

Proof. Since z and y commute, y and yz have the same order and $y^{p^m} = (yz)^{p^m}$. The map α can thus be extended to an endomorphism of P. It is clear that α is surjective, so that α is a well-defined automorphism of P.

Since $\alpha^{p^k}(y) = yz^{p^k}$, then $\alpha^{p^k}y = y$ if and only if $k \geq m$. Hence, α has order p^m. $\square$

Definition 1.4.8. Let $m \geq 1$. For $s \leq m$, we define $M(m, s)$ as the semi-direct product $(C_{p^{m+s}} \underset{C_{p^s}}{*} C_{p^m}) \underset{\alpha}{\rtimes} C_{p^m}$, where α is the automorphism defined in Lemma 1.4.7. For $s \geq m$, we define $M(m, s)$ as the semi-direct product $C_{p^{m+s}} \rtimes C_{p^m}$, with respect to the automorphism sending a generator y of $C_{p^{m+s}}$ to y^{1+p^s}.

The group $M(m, s)$ has the following presentations. If $s \leq m$, then

$$\begin{aligned} M(m,s) &= \langle x, y \,|\, x^{p^m} = y^{p^{m+s}} = 1, y^{p^m} = [x,y]^{p^{m-s}}, [x,[x,y]] = [y,[x,y]] = 1\rangle \\ &= \langle x, y, z \,|\, x^{p^m} = z^{p^m} = 1, y^{p^m} = z^{p^{m-s}}, z = [x,y], [x,z] = [y,z] = 1\rangle, \end{aligned}$$

and if $s \geq m$, then

$$\begin{aligned} M(m,s) &= \langle x, y \,|\, x^{p^m} = y^{p^{m+s}} = 1, y^{p^s} = [x,y]\rangle \\ &= \langle x, y, z \,|\, x^{p^m} = y^{p^{m+s}} = 1, z = y^{p^m}, [x,y] = z^{p^{s-m}}\rangle. \end{aligned}$$

Remark 1.4.9.

a) If $s = m$, then $C_{p^{m+s}} \underset{C_{p^s}}{*} C_{p^m} = C_{p^{m+s}}$ and the two definitions coincide.

b) Let $P = M(m, s)$ with either $s \leq m$, or $s \geq m$. In both cases, m is the p-valuation of the order of P' and we will see in Lemma 1.4.10 that s is the p-valuation of the order of the cyclic group $\mho^m(P)$.

c) When $m = 1$, the group $M(1, s)$ is isomorphic to the group $M_{p^{s+2}}$ that appeared in previous Section 1.3.

d) If $s = 0$, then $M(m, 0) = X_3(p^m)$.

e) We don't want to use a notation of the form $M_r(p^m)$ for some index r, because one would maybe expect then the order of this group to be p^{mr}. But we will see in the next lemma that the order of the groups $M(m, s)$ are really different whether s is less or greater than m. Our notation doesn't correspond nicely with our previous notation for $m = 1$, but it seems to us that it is less confusing this way.

Lemma 1.4.10. *If $P = M(m,s)$, then*

a) $P/Z(P)$ is isomorphic to $C_{p^m} \times C_{p^m}$,

b) $\mho^m(P)$ is cyclic of order p^s,

c) P' is cyclic of order p^m,

d) $Z(P)$ is cyclic of order $p^{\max\{m,s\}}$,

e) P has order $p^{2m+\max\{m,s\}}$.

Proof. We keep the notation as in the above presentations. If $s \leq m$, then $Z(P)$ is generated by $[x,y]$, hence has order p^m. If $s \geq m$, then $Z(P)$ is generated by y^{p^m}, hence has order p^s. The other properties follow easily. $\square$

In Figure 1.3 and Figure 1.4, we have shown some of the subgroups of the group $M(m,s)$. The letters x and y refer to the above presentations and we have labelled (some of) the edges with the p-valuation of the indices.

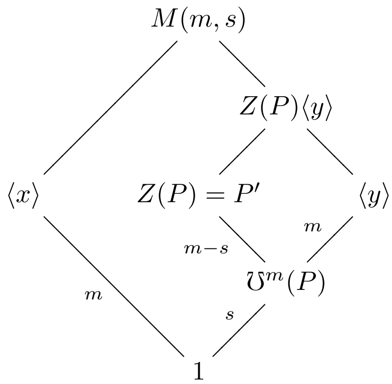

Figure 1.3: Some of the structure of the group $M(m,s)$ for $s \leq m$

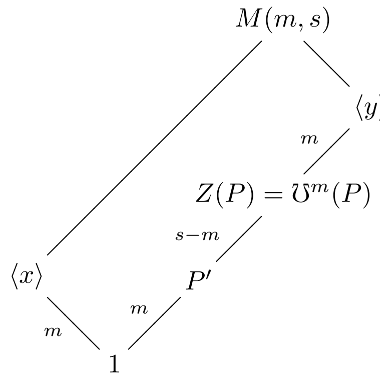

Figure 1.4: Some of the structure of the group $M(m,s)$ for $s \geq m$

Recall that, for $m \geq 1$ and $s \geq 0$, the center of $M(m,s)$ has order $p^{\max\{m,s\}}$. For $r \geq 0$, we can then form the central product $M(m,s) * C_{p^{m+r}}$, where the amalgamation is performed over the largest central subgroup possible. It may well be that different choices of the values of m, r and s give isomorphic groups $M(m,s) * C_{p^{m+r}}$. This is the content of the following lemma.

Lemma 1.4.11. *Let $P = M(m,s) * C_{p^{m+r}}$, with $m \geq 1$, $s \geq 0$ and $r \geq 0$. Then one of the following situations arises.*

a) $m + r \leq \max\{m,s\}$, and then P is isomorphic to $M(m,s)$.

b) $0 < r$ and $s \leq r$, and then P is isomorphic to $X_3(p^m) * C_{p^{m+r}}$.

c) $0 < r < s < m + r$, and then $P = M(m,s) * C_{p^{m+r}}$.

Furthermore, under the given conditions, no two of these groups are isomorphic.

Proof. If $r = 0$, then $m + r = m \leq \max\{m,s\}$, so that m, r and s satisfy the condition of a). From now on, we suppose $r > 0$.

If $s \leq m$, then $s < m + r$ and we have either $s \leq r$, in which case the conditions of b) are satisfied, or $r < s$, in which case $0 < r < s < m + r$, so that the conditions of c) are satisfied.

If $s \geq m$, then either $m+r \geq s = \max\{m,s\}$ (conditions of a)), or $s < m+r$. In this second case, we have either $s \leq r$ (conditions of b)), or $r < s$ (conditions of c)).

In all cases, m, r and s satisfy one of the three conditions. It remains to show, for each of these conditions, that P is isomorphic to the corresponding group.

If $m + r \leq \max\{m,s\}$, the whole group $C_{p^{m+r}}$ is amalgamated along the center of $M(m,s)$, so that $P \cong M(m,s)$. It follows from Lemma 1.4.10 that in this situation, $Z(P)$ has order $p^{\max\{m,s\}}$ and $|\mho^m(P)|$ has order p^s.

Suppose now $r > 0$ and $r \geq s$. The condition $s \leq r$ implies in particular $s < m + r$, so that the amalgamation is performed along the subgroup of order $p^{\max\{m,s\}}$. Let y be a generator of $M(m,s)$ of order p^{m+s}. One the one hand, we have that y^{p^m} is in the center of $M(m,s)$ and has order p^s. On the other hand, if z is a generator of the subgroup $C_{p^{m+r}}$, then $z^{p^{m+r-s}}$ has order p^s (note that $m + r - s > 0$). Because of the way the amalgamation is performed, we have that y^{p^m} and $z^{p^{m+r-s}}$ lie in a common subgroup of order p^s. It follows that $y^{p^m} = (z^{p^{m+r-s}})^k$, for some k prime to p. But since $s \leq r$, we also have $(z^{p^{m+r-s}})^k = (z^{kp^{r-s}})^{p^m}$. Now letting $y' = yz^{-kp^{r-s}}$, we have

$$(y')^{p^m} = (yz^{-kp^{r-s}})^{p^m} = y^{p^m}(z^{p^{m+r-s}})^{-k} = 1.$$

If we replace y by y', we may assume that $y^{p^m} = 1$, so that $P = X_3(p^m) * C_{p^{m+r}}$. Because of the way the amalgamation is performed, we have that $Z(P)$ is generated by z, i.e. $Z(P)$ has order p^{m+r}. In the group $X_3(p^m) * C_{p^{m+r}}$, the subgroup $\mho^m(P)$ is generated by z^{p^m}, hence is cyclic of order p^r.

Suppose finally $0 < r < s < m + r$. The center of $M(m,s)$ is wholly amalgamated in the subgroup $C_{p^{m+r}}$, hence $Z(P) = C_{p^{m+r}}$. Let z be a generator of the subgroup $C_{p^{m+r}}$ and let y be a generator of $M(m,s)$ of order p^{m+s}. The subgroup $\mho^m(P)$ is generated by y^{p^m}, which has order p^s, and z^{p^m}, which has order p^r. Since $s > r$, the subgroup $\mho^m(P)$ is then generated by y^{p^m}, hence is cyclic of order p^s.

It is enough to compare the order of the center and of $\mho^m(P)$ in each of the three cases to show that these groups are non-isomorphic under the given conditions. $\square$

Recall that p is an odd prime and that P is a p-group of class 2 with a cyclic center. We also have, by assumption, that the quotient group $L = P/Z(P)$ is homocyclic of type p^m. If R denotes the ring $\mathbb{Z}/p^m\mathbb{Z}$, then L is a free R-module and the choice of a generator u of P' induces an isomorphism $P' \cong R$. The commutators induce a regular alternating form

$$b : L \times L \to R,$$

so that L is a regular alternating space over $R = \mathbb{Z}/p^m\mathbb{Z}$. We have that $Z(P)$ is cyclic and contains P', hence $Z(P)$ has order p^{m+r} for some $r \geq 0$. Let z be a generator of $Z(P)$ such that $z^{p^r} = u$. Taking p^m-th powers induces a well-defined map

$$\varphi : L \to Z(P)/\mho^m(Z(P)).$$

The quotient group $Z(P)/\mho^m(Z(P))$ is cyclic of order p^m and there is an isomorphism $Z(P)/\mho^m(Z(P)) \cong R$, sending the class of z to $1 \in R$. If we identify the quotient $Z(P)/\mho^m(Z(P))$ with R, then we can see φ as a map

$$\varphi : L \to R,$$

and Lemma 1.4.2 shows that φ is linear. With these information, we are now in position to state the following proposition, classifying odd order p-groups of class 2 with a cyclic center and whose quotient by the center is homocyclic.

Proposition 1.4.12. *Let p be an odd prime and let P be a non-abelian p-group of class 2 with a cyclic center and suppose that $P/Z(P)$ is homocyclic of type p^m with $m \geq 1$. Let p^s be the order of $\mho^m(P)$. Then $P/Z(P)$ has order $p^{2\ell m}$, for some $\ell \geq 1$ and P is isomorphic to one of the following groups:*

1. *$P = X_{2\ell+1}(p^m)$.*
2. *$P = X_{2\ell+1}(p^m) * C_{p^{m+r}}$ with $r \geq 1$.*
3. *$P = X_{2\ell-1}(p^m) * M(m, s)$ for some $s \geq 1$.*
4. *$P = X_{2\ell-1}(p^m) * M(m, s) * C_{p^{m+r}}$ with $1 \leq r < s < m + r$.*

Furthermore, under the given conditions, no two of these groups are isomorphic.

Proof. Let $|Z(P)| = p^{m+r}$. We have just seen that the commutators induce a regular alternating form b on $L = P/Z(P)$, which is a free module over $R = \mathbb{Z}/p^m\mathbb{Z}$. Taking p^m-th powers in turn induces a linear map $\varphi : L \to R$. Lifting to P the elements of a symplectic basis given by Lemma A.0.15 shows that P is generated by the generator z of $Z(P)$ and elements $x_1, y_1, \ldots, x_\ell, y_\ell$ satisfying

$$[x_i, y_i] = z^{p^r}, \tag{1.21}$$

$$[x_i, y_j] = [x_i, x_j] = [y_i, y_j] = 1, \text{ for } i \neq j, \tag{1.22}$$

$$x_j^{p^m}, y_j^{p^m}, x_\ell^{p^m} \in \mho^m(Z(P)), \text{ for all } j = 1, \ldots, \ell - 1, \tag{1.23}$$

$$y_\ell^{p^m} \in z^{p^a}\mho^m(Z(P)), \text{ for some } 0 \leq a \leq m. \tag{1.24}$$

The subgroup $\mho^m(Z(P))$ is generated by z^{p^m}, so that $x_\ell^{p^m} = z^{kp^m}$ for some k. If we replace x_ℓ by $x_\ell z^{-k}$, we see that we can assume that $x_\ell^{p^m} = 1$. A similar argument shows that we can also assume that $x_i^{p^m} = y_i^{p^m} = 1$, for all $i = 1, \ldots, \ell - 1$, and that $y_\ell^{p^m} = z^{p^a}$.

Let X denote the subgroup of P generated by the elements x_j, y_j, for $j = 1, \cdots, \ell - 1$. Let also M denote the subgroup generated by x_ℓ and y_ℓ. In view of what preceeds, P is a central product $P = X * M * Z(P)$, the subgroup X is isomorphic to $X_{2(\ell-1)+1}(p^m)$ and the subgroup M is isomorphic to $M(m, s')$, where $s' = m + r - a$. Furthermore, $M * Z(P)$ is then isomorphic to a central product $M(m, s') * C_{p^{m+r}}$.

Suppose first $a = m$. In this situation, $y_\ell^{p^m}$ is in the subgroup generated by z^{p^m}, so that we may assume that $y_\ell^{p^m} = 1$. The subgroup M is thus isomorphic to $X_3(p^m)$.

If we have in additition that $r = 0$, then we have also $s' = r = 0$ and hence $m + r = m \leq \max\{m, s'\} = m$. It follows then from Lemma 1.4.11, that $M * Z(P)$ isomorphic to $X_3(p^m)$, and hence P is isomorphic to $X_{2\ell+1}(p^m)$. This is the first case of our statement. In this case, $Z(P) = P'$ has order p^m and $\mho^m(P)$ is trivial, so that in particular $s' = s = 0$.

If $r > 0$, then $M * Z(P)$ is isomorphic to $X_3(p^m) * C_{p^{m+r}}$, with $m + r > m$. It follows that $P = X_{2\ell+1}(p^m) * C_{p^{m+r}}$, with $r \geq 1$. This is the second case of our statement. In this case, $Z(P)$ has order p^{m+r}, with $m + r > m$, and $\mho^m(P)$ has order p^r, with $r > 0$. In particular, $s = r$ by the definition of s and $s' = m + r - a = r$, since $a = m$, so that also $s' = s$.

Suppose from now on that $a < m$. If, in addition, $m + r \leq \max\{m, s'\}$, then $M * Z(P) = M(m, s') * C_{p^{m+r}}$ is isomorphic to $M(m, s')$, by Lemma 1.4.11. This is the third case of our statement. In this case, $P = X * (M * Z(P))$ is isomorphic to $X_{2\ell-1}(p^m) * M(m, s')$. In particular, $Z(P)$ has order $p^{\max\{m,s'\}}$ and $\mho^m(P)$ has order $p^{s'}$, so that also $s' = s$.

Remark that $a < m$ implies in particular $s' = m + r - a > r$, so that if $m + r > \max\{m, s'\}$, then it follows from Lemma 1.4.11, that P is isomorphic to $X_{2\ell-1}(p^m) * M(m, s') * C_{p^{m+r}}$, with $0 < r < s' < m + r$. This is the fourth case in our statement. In this case, $Z(P)$ has order p^{m+r} and $\mho^m(P)$ has order $p^{s'}$, so that also $s' = s$.

By considering the order of the subgroups $Z(P)$ and $\mho^m(P)$ in the four cases, it is not difficult to see that these four groups are non-isomorphic under the given conditions. □

Remark 1.4.13. If $m = 1$, then $M(m, s) = M(1, s) = M_{p^{s+2}}$ and there are no choices of s such that $1 \leq r < s < m + r$. It follows that the fourth case of the above proposition does not arise and we recover then the classification of odd order p-groups with a cyclic center and a central Frattini subgroup.

The general case

Recall that p is an odd prime and let P be a p-group of class 2 with a cyclic center (with $P/Z(P)$ not necessarily homocyclic). Let $p^m = |P'|$, it follows from Lemma 1.4.1 that $P/Z(P)$ has exponent p^m. In particular, if R denotes the ring $\mathbb{Z}/p^m\mathbb{Z}$, then P' can be identified with R, and $M = P/Z(P)$ can be seen as an R-module. As usual, the commutators induce a regular alternating form

$$b : M \times M \to R.$$

For $m_i \leq m$, let $\tau_i : \mathbb{Z}/p^{m_i}\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ be the canonical injection given by multiplication by p^{m-m_i}. Following Proposition A.0.16, we have that M can be decomposed as an orthogonal sum $M = (M_1, b_1) \oplus \cdots \oplus (M_t, b_t)$, where each (M_i, b_i) is a regular alternating space over some ring $\mathbb{Z}/p^{m_i}\mathbb{Z}$ and the restriction b_{M_i} of b to M_i is equal to $\tau_i b_i$. The meaning of this last condition should become clear in the course of the proof of the following proposition.

Proposition 1.4.14. *Let p be an odd prime and let P be a non-abelian p-group of class 2 with a cyclic center. Let $p^m = |P'|$ and $p^{m+r} = |Z(P)|$. Then P is a central product $P = Q_1 * \cdots * Q_t * Z(P)$, where each quotient $Q_i/Z(Q_i)$ is homocyclic of type p^{m_i}. Furthermore, for each $i = 1, \ldots, t$, there exists $\ell_i \geq 1$ such that Q_i is isomorphic either to $X_{2\ell_i+1}(p^{m_i})$, or to $X_{2\ell_i-1}(p^{m_i}) * M(m_i, s_i)$ with $0 < m + r - m_i < s_i < m + r$.*

Proof. Keeping the notation as above, we let $S_i/Z(P) = M_i$. The decomposition of M as the orthogonal sum $\bigoplus M_i$ implies that P decomposes as a central product $P = S_1 * \cdots * S_t$. Note that this implies in particular that $Z(S_i) = Z(P)$. Since M_i is free over $\mathbb{Z}/p^{m_i}\mathbb{Z}$, we have that $S_i/Z(P) = S_i/Z(S_i)$ is homocylic of type p^{m_i}.

The map b induced by commutators restricts to M_i giving an alternating form

$$b_{M_i} : M_i \times M_i \to P' \cong \mathbb{Z}/p^m\mathbb{Z}.$$

Unless if $m_i = m$, the pair (M_i, b_{M_i}) is not an alternating space. However, it follows from Lemma 1.4.1, that $[S_i, S_i]$ has order p^{m_i}, i.e. is the cyclic subgroup of $Z(P)$ of order p^{m_i}.

If z is a generator of $Z(P)$, then $u = z^{p^r}$ is a generator of P' and $u^{p^{m-m_i}}$ is a generator of $[S_i, S_i]$. This induces an isomorphism $[S_i, S_i] \cong \mathbb{Z}/p^{m_i}\mathbb{Z}$ and taking commutators in S_i induces then an alternating form

$$b_i' : M_i \times M_i \to \mathbb{Z}/p^{m_i}\mathbb{Z} \cong \langle u^{p^{m-m_i}} \rangle.$$

The condition $b_{M_i} = \tau_i b_i$ implies that $[x, y] = (u^{p^{m-m_i}})^{b_i(\overline{x}, \overline{y})}$, for all $x, y \in S_i$. We have therefore that $b_i' = b_i$ and thus b_i' is regular.

We have thus obtained subgroups $S_1, \ldots, S_t$ of P satisfying the following conditions

1. $P = S_1 * \cdots * S_t$.
2. $Z(S_i) = Z(P)$.
3. $M_i = S_i/Z(S_i)$ is a free $\mathbb{Z}/p^{m_i}\mathbb{Z}$-module endowed with the non-degenerate alternating form $b_i : M_i \times M_i \to \mathbb{Z}/p^{m_i}\mathbb{Z} \cong \langle u^{p^{m-m_i}} \rangle$ induced by taking commutators in S_i.

Remark that $Z(S_i)$ has order p^{m+r} and $[S_i, S_i]$ has order p^{m_i}. It follows that $Z(S_i)$ has order $p^{m_i+r_i}$, where $r_i = m + r - m_i$. Proposition 1.4.12 implies thus that the subgroup S_i can be written as $S_i = Q_i * Z(P)$, where Q_i is isomorphic either to $X_{2\ell_i+1}(p^m)$, or to a central product $X_{2\ell_i-1}(p^{m_i}) * M(m_i, s_i)$ with the conditions $0 < r_i = m + r - m_i < s_i < m + r$. The proposition follows now from the equality

$$(Q_1 * Z(P)) * \cdots * (Q_t * Z(P)) = Q_1 * \cdots * Q_t * Z(P).$$

□

Corollary 1.4.15. *Let p be an odd prime and let P be a non-abelian p-group of class 2 with a cyclic center. Let $p^m = |P'|$ and $p^{m+r} = |Z(P)|$. Then P is isomorphic to a central product*

$$X_{2\ell_{\alpha_1}+1}(p^{m_{\alpha_1}}) * \cdots * X_{2\ell_{\alpha_h}+1}(p^{m_{\alpha_h}}) * M(m_{\beta_1}, s_{\beta_1}) * \cdots * M(m_{\beta_k}, s_{\beta_k}) * C_{p^{m+r}}$$

where $h, k \geq 0$ with $(h, k) \neq (0, 0)$, $\ell_{\alpha_i} > 0$ and the following conditions are satisfied:

1. $m_{\alpha_1} > \cdots > m_{\alpha_h} > 0$.
2. $m_{\beta_1} > \cdots > m_{\beta_k} > 0$.
3. $m = \max\{m_{\alpha_1}, m_{\beta_1}\}$.
4. $0 < m + r - m_{\beta_j} < s_{\beta_j} < m + r$.

We briefly explain the meaning of the various conditions in the previous corollary. The condition $(h, k) \neq (0, 0)$ ensures that P is not abelian. The first two conditions in the list just say that we have chosen to order the factors of the central product. Since P' is generated by the derived subgroups of the factors of the central product, we must have that at least one of the factors has a derived subgroup of order p^m. But the order of the derived subgroup of a factor is the corresponding m_{α_i} or m_{β_j}. Because of the ordering this must be m_{α_1} or m_{β_1}.

The fourth condition of the list, namely $0 < m + r - m_{\beta_j} < s_{\beta_j} < m + r$, ensures that we cannot use the center to modify the order of the generators of the group $M(m_{\beta_j}, s_{\beta_j})$. It may however be possible to modify these generators with an element of one of the other factors of the central product. There are thus no reasons for this decomposition to be canonical in the sense that a p-group may have several such decompositions. We would like to give an overview of how this isomorphism problem can be solved. This is done essentially in the following lemma. The proof consists in modifying generators in a way similar (but more complicated) to what we have performed in Lemma 1.4.11. In what follows, the central products are always performed over the largest subgroup possible.

Lemma 1.4.16. *Let m_1, s_1, m_2, s_2 such that $m_1 \geq m_2 > 0$ and $s_1, s_2 \geq 0$.*

a) If $m_1 \geq m_2 + s_2$ then $M(m_1, s_1) * M(m_2, s_2) \cong M(m_1, s_1) * X_3(p^{m_2})$.

b) If $s_1 \geq s_2$ then $M(m_1, s_1) * M(m_2, s_2) \cong M(m_1, s_1) * X_3(p^{m_2})$.

c) If $m_2 + s_2 \geq m_1 + s_1$ then $M(m_1, s_1) * M(m_2, s_2) \cong X_3(p^{m_1}) * M(m_2, s_2)$.

Proof. For $i = 1, 2$, let M_i be the group $M(m_i, s_i)$ and let x_i, y_i be generators of M_i with x_i of order p^{m_i} and y_i of order $p^{m_i+s_i}$. Denote by Q the central product $Q = M_1 * M_2 = M(m_1, s_1) * M(m_2, s_2)$.

Recall that, for $i = 1, 2$, the center of $M_i = M(m_i, s_i)$ has order $p^{\max\{m_i, s_i\}}$. Because of the way the amalgamation is performed, it follows that $y_i^{p^k}$ is in $M_1 \cap M_2$, if the order of $y_i^{p^k}$ is at most $\min\left\{p^{\max\{m_1,s_1\}}, p^{\max\{m_2,s_2\}}\right\}$. The same holds for elements of the form $[x_i, y_i]^{p^k}$.

Suppose first $m_1 \geq m_2 + s_2$. This implies in particular $m_1 \geq s_2$ and since $m_1 \geq m_2$, the cyclic subgroups of order p^{s_2} in $Z(M_1)$ and $Z(M_2)$ are amalgamated in $M_1 \cap M_2$. It follows that the element $y_2^{p^{m_2}}$ is in $M_1 \cap M_2$, since it has order p^{s_2} and is in $Z(M_2)$. The element $u = [x_1, y_1]^{p^{m_1-(m_2+s_2)}}$ has order $p^{m_2+s_2}$ and is in $Z(M_1)$, hence $u^{p^{m_2}}$ has order p^{s_2} and is in $M_1 \cap M_2$. We have thus

$$y_2^{p^{m_2}} = (u^{p^{m_2}})^k = u^{kp^{m_2}},$$

for some k prime to p. If we set $y_2' = y_2 u^{-k}$, then $(y_2')^{p^{m_2}} = 1$, so that $\langle x_2, y_2' \rangle$ is isomorphic to $X_3(p^{m_2})$. Since u is central in M_1 and hence in Q, we have now $Q = M_1 * \langle x_2, y_2' \rangle = M(m_1, s_1) * X_3(p^{m_2})$.

Suppose now $s_1 \geq s_2$. Since $m_1 \geq m_2$ by assumption, we have in particular that the intersection $M_1 \cap M_2$ has order $p^{\max\{m_2,s_2\}}$. The element $y_2^{p^{m_2}}$ has order p^{s_2} and is in $Z(M_2)$, hence is in $M_1 \cap M_2$. Since $m_1 \geq m_2$ and $s_1 \geq s_2$, we have $m_1 + s_1 \geq m_2 + s_2$ and we let

$$u = y_1^{p^{(m_1+s_1)-(m_2+s_2)}}.$$

The element $u^{p^{m_2}} = y_1^{p^{(m_1+s_1)-s_2}}$ has order p^{s_2} and is in $Z(M_1)$ since we have $m_1 + (s_1 - s_2) \geq m_1$, and hence $u^{p^{m_2}}$ is in $M_1 \cap M_2$. We have thus

$$y_2^{p^{m_2}} = (u^{p^{m_2}})^k = u^{kp^{m_2}},$$

for some k prime to p. If we set

$$y_2' = y_2 u^{-k} = y_2 y_1^{-kp^{(m_1+s_1)-(m_2+s_2)}},$$

then $(y_2')^{p^{m_2}} = 1$. Remark that $[x_2, y_2'] = [x_2, y_2]$, since y_1 centralizes x_2. We have also $[y_1, y_2'] = [y_1, y_2] = 1$, but we don't have necessarily that $[x_1, y_2']$ is trivial. Since y_2 commutes with both x_1 and u, we have

$$[x_1, y_2'] = [x_1, y_2 u^{-k}] = [x_1, u^{-k}] = [x_1, y_1]^{-kp^{(m_1+s_1)-(m_2+s_2)}}.$$

If $(m_1+s_1)-(m_2+s_2)\geq m_1$, i.e. $m_2+s_2\leq s_1$, then $[x_1,y_2']=1$, since $[x_1,y_1]$ has order p^{m_1}. In this case, $Q=M_1*\langle x_2,y_2'\rangle\cong M(m_1,s_1)*X_3(p^{m_2})$.

If $(m_1+s_1)-(m_2+s_2)<m_1$, i.e. $m_2+s_2>s_1$, we show how to modify x_1 to recover a central decomposition of Q. Since k is prime to p, we have that $[x_1,y_1]^{-kp^{(m_1+s_1)-(m_2-s_2)}}$ has order $p^{(m_2+s_2)-s_1}$ and is in $M_1\cap M_2$, since $m_2+(s_2-s_1)\leq m_2$. There exists thus r such that

$$[x_1,y_1]^{-kp^{(m_1+s_1)-(m_2-s_2)}}=[x_2,y_2]^r.$$

We let

$$x_1'=x_1x_2^{-r},$$

and we obtain $[x_1',y_2']=1$. If we let $M_1'=\langle x_1',y_1\rangle$ and $M_2'=\langle x_2,y_2'\rangle$, we have then $Q=M_1'*M_2'$ and M_2' is isomorphic to $X_3(p^{m_2})$, so that $Q=M(m_1,s_1)*X_3(p^{m_2})$.

Suppose finally $m_2+s_2\geq m_1+s_1$. Remark that since $m_1\geq m_2$, we have in particular $s_1\leq s_2$. It follows that the subgroups of order p^{s_1} of $Z(M_1)$ and $Z(M_2)$ are amalgamated in $M_1\cap M_2$. The element $y_1^{p^{m_1}}$ has order p^{s_1} and is in $Z(M_1)$, hence in $M_1\cap M_2$.

Let $u=y_2^{p^{(m_2+s_2)-(m_1+s_1)}}$, the element $u^{p^{m_1}=y_2^{p^{(m_2+s_2)-s_1}}}$ has order p^{s_1} and is in $Z(M_2)$, since $m_2+(s_2-s_1)\geq m_2$, hence is in $M_1\cap M_2$. We have thus

$$y_1^{p^{m_1}}=(u^{p^{m_1}})^k=u^{kp^{m_1}},$$

for some k prime to p. If we set

$$y_1'=y_1u^{-k}=y_1y_2^{-kp^{(m_2+s_2)-(m_1+s_1)}},$$

then $(y_1')^{p^{m_1}}=1$. Remark that $[x_1,y_1']=[x_1,y_1]$ and $[y_2,y_1]=1$. Furthermore, we have

$$[x_2,y_1']=[x_2,y_1u^{-k}]=[x_2,y_2]^{-kp^{(m_2+s_2)-(m_1+s_1)}}.$$

If $(m_2+s_2)-(m_1+s_1)\geq m_2$, i.e. $s_2\geq(m_1+s_1)$, then $[x_2,y_1']=1$, since $[x_2,y_2]$ has order p^{m_2}. In this case, we have $Q=\langle x_1,y_1'\rangle*M_2\cong X_3(p^{m_1})*M(m_2,s_2)$.

If $(m_2+s_2)-(m_1+s_1)<m_2$, i.e. $s_2<(m_1+s_1)$, then the element $[x_2,y_2]^{-kp^{(m_2+s_2)-(m_1+s_1)}}$ has order $p^{(m_1-s_1)-s_2}$, since k is prime to p. Since $(m_1+s_1)-s_2\leq m_2\leq m_1$, there exists r such that

$$[x_2,y_2]^{-kp^{(m_2+s_2)-(m_1+s_1)}}=[x_1,y_1]^r.$$

We let

$$x_2'=x_2x_1^{-r},$$

so that $[x_1',y_2']=1$. We have this way that $Q=\langle x_1,y_1'\rangle*\langle x_2'y_2\rangle$ is isomorphic to $X_3(p^{m_1})*M(m_2,s_2)$ and the lemma is proved. □

Putting together Corollary 1.4.15 and Lemma 1.4.16 we obtain the following theorem, due originally to [9] and [19] but with a different approach.

Theorem 1.4.17. *Let p be an odd prime. If P is a p-group of class 2 with a cyclic center, then P is isomorphic to a central product*

$$X_{2\ell_{\alpha_1}+1}(p^{m_{\alpha_1}})*\cdots*X_{2\ell_{\alpha_r}+1}(p^{m_{\alpha_r}})*M(m_{\beta_1},s_{\beta_1})*\cdots*M(m_{\beta_t},s_{\beta_t})*C_{p^n}$$

with $\ell_{\alpha_i}>0$ and the following conditions:

1. $m_{\alpha_1} > m_{\alpha_2} > \ldots > m_{\alpha_r} > 0$;

2. $n > m_{\beta_1} > m_{\beta_2} > \ldots > m_{\beta_r}$;

3. $m_{\beta_1} + s_{\beta_1} > m_{\beta_2} + s_{\beta_2} > \ldots > m_{\beta_t} + s_{\beta_t} > n$;

4. $m_{\beta_t} + s_{\beta_t} > m_{\beta_1}$

5. $n > s_{\beta_t} > s_{\beta_{t-1}} > \ldots > s_{\beta_1} > 0$.

Furthermore each P has a unique such decomposition satisfying the given conditions.

The existence of the decomposition follows from the previous decomposition obtained in 1.4.15 to which we apply Lemma 1.4.16. This lemma should already give a good idea to the reader on why this decomposition is unique and we will not say more on the proof of this fact. For a detailed proof the reader can refer to the work of Leong [19]. Since we don't use the same notation as Leong , let us just mention that our group $M(m, s)$ is equal to the group $Q(\alpha, \beta)$ of Leong by setting $\alpha = m + s$ and $\beta = m$.

Additional remarks

Our first remark concerns the importance of the assumption that $Z(P)$ is cyclic in the above classification. Let Q be a p-group of class 2 with cyclic derived subgroup. If A is an abelian p-group, then the group $P = Q \times A$ has class 2, $P' = Q'$ and $Z(P) = Z(Q) \times A$. In some sense, one can always "add" an abelian p-group to the center. But contrary to the case of p-groups with cyclic Frattini subgroup, the reverse operation is not always possible. This can be seen in the following example.

Example 1.4.18. Let $H = C_{p^2} \times C_{p^3} \times C_p$ with generators y of order p^2, r of order p^3 and s of order p. The group H has an automorphism α of order p^2 which fixes r and s and sends y to $r^p sy$. Let P be the semi-direct product of a cyclic group of order p^2 generated by x acting on H with respect to α. It is not difficult to see that P' is cyclic of order p^2 and generated by $r^p s$ and that $Z(P)$ is abelian of type (p^3, p) generated by r and s.

Suppose that P can be written as a direct product $P = Q \times A$ with A abelian and $Z(Q)$ cyclic. One the one hand $P' \leq Q' \leq Q$, but on the other hand P' is central in P, so that $P' \leq Z(Q)$. In particular, $|Z(Q)| \geq p^2$ and since $Z(P) = Z(Q) \times A$ has type (p^3, p) we have that $Z(Q)$ is cyclic of order p^3 and A is cyclic of order p. Now, this means that there exists $z \in Z(Q) \leq Z(P)$ such that $z^p = r^p s$. But this is a contradiction, since in $Z(P)$ all p-th powers lie in the subgroup generated by r.

Our second remark concerns the case $p = 2$. We give first the analogue of Lemma 1.4.1 and Lemma 1.4.2 for $p = 2$. The proof of Lemma 1.4.1 works for $p = 2$ with no restriction, so that we obtain the following lemma.

Lemma 1.4.19. *If P is a 2-group of class 2 with cyclic center, then $P/Z(P)$ has exponent 2^m if and only if P' has order 2^m.*

Lemma 1.4.20. *Let P be a 2-group of class 2 with cyclic center and $|P'| = 2^m$. Then for all $x, y \in P$,*

$$(xy)^{2^m} = [x, y]^{2^{m-1}} x^{2^m} y^{2^m}.$$

Proof. Since $P' \leq Z(P)$, we have

$$(xy)^{2^m} = [y, x]^{\frac{2^m(2^m-1)}{2}} x^{2^m} y^{2^m} = [x, y]^{2^{m-1}} x^{2^m} y^{2^m}.$$

□

Suppose that P is a 2-group of class 2 with cyclic center and such that $V = P/Z(P)$ is homocyclic of type 2^m. Let φ be the map

$$\varphi : V \to Z(P)/\mho^m(Z(P)) \cong \mathbb{Z}/2^m\mathbb{Z}$$

induced by taking 2^m-th powers. Lemma 1.4.20 shows that the map φ will not be linear in general, because of the term $[x, y]^{2^{m-1}}$. But for $x, y \in P$, this element $[x, y]^{2^{m-1}}$ is in the unique subgroup of order 2 of $Z(P)$, hence is contained in $\mho^m(Z(P))$ at the condition that $Z(P)$ has order strictly greater than 2^m, i.e. if P' is strictly contained in $Z(P)$. This proves the following lemma.

Lemma 1.4.21. *If P' is strictly contained in $Z(P)$, then φ is linear.*

Similarly to the case p odd, we can define the groups $X_3(2^m)$ by

$$X_3(2^m) = \langle x, y \,|\, x^{2^m} = y^{2^m} = 1, [x, y]^{2^m} = 1, [x, [x, y]] = [y, [x, y]] = 1\rangle.$$

We define also the groups $M(m, s)$ by

a) If $s \leq m$, then

$$M(m, s) = \langle x, y \,|\, x^{2^m} = y^{2^{m+s}} = 1, y^{2^m} = [x, y]^{2^{m-s}}, [x, [x, y]] = [y, [x, y]] = 1\rangle.$$

b) If $s \geq m$, then

$$M(m, s) = \langle x, y \,|\, x^{2^m} = y^{2^{m+s}} = 1, y^{2^s} = [x, y]\rangle.$$

The group $X_{2^{\ell+1}}(2^m)$ is then defined as the central product of ℓ copies of the group $X_3(2^m)$. The following result follows now from the general results on linear form on alternating free $\mathbb{Z}/2^m\mathbb{Z}$-modules (see Lemma A.0.15). The proof is similar to the case p odd.

Proposition 1.4.22. *Let P be a 2-group of class 2 with a cyclic center and such that $P/Z(P)$ is homocyclic of type 2^m, for some $m \geq 1$. We assume that P' is strictly contained in $Z(P)$ and let $2^s = |\mho^m(P)|$. Then P is isomorphic to a central product $X_{2\ell+1}(2^m) * S$, where S is either cyclic of order 2^{m+r} with $r \geq 1$, isomorphic to $M(m, s)$ with $s > m$, or isomorphic to $M(m, s) * C_{2^{m+r}}$ for some $1 < r < s < m + r$.*

When P' is equal to $Z(P)$, then the map φ is not linear anymore. This is not even a quadratic form on the ring $\mathbb{Z}/2^m\mathbb{Z}$, since $\varphi(k\cdot v) = k\cdot\varphi(v)$. However, the map induced by the commutators is still a non-degenerate alternating form on $V = P/Z(P)$. In particular, we can lift to P the elements of a symplectic basis and then the order of the elements can be modified directly in the group. We introduce one more 2-group of class 2,

$$Q(m) = \langle x, y \,|\, x^{2^{m+1}} = 1, x^{2^m} = y^{2^m} = [x,y]^{2^{m-1}}, [x,[x,y]] = [y,[x,y]] = 1\rangle.$$

For $m = 1$, $Q(1)$ is the quaternion group of order 8.

Proposition 1.4.23. *Let P be a 2-group of class 2 with cyclic center and such that $P/Z(P)$ is homocyclic of type 2^m. Assume also that $P' = Z(P)$. Then P is isomorphic to a central product $X_{2\ell+1}(2^m) * S$, where S is either trivial, isomorphic to $M(m,s)$ for some $1 \leq s \leq m$, or isomorphic to the group $Q(m)$.*

Proof. Let $e_1, f_1, \ldots, e_\ell, f_\ell$ be a symplectic basis of $P/Z(P)$. Let x_i, respectively y_i, be a representative of e_i, resp. f_i. If $x_i^{2^m} = y_i^{2^m} = 1$ for all $i = 1, \ldots, \ell$, then P is isomorphic to $X_{2^{\ell+1}}(2^m)$. Suppose now that there exists k such that $x_k^{2^m} \neq 1$ or $y_k^{2^m} \neq 1$. Without loss of generality, we may assume that $y_\ell^{2^m} \neq 1$ and that $y_\ell^{2^m}$ has maximal order among the set $\{x_i^{2^m}, y_i^{2^m}, i = 1, \ldots, \ell\}$.

In particular, $x_\ell^{2^m}$ and the elements $x_j^{2^m}, y_j^{2^m}$, for $1 \leq j \leq \ell - 1$ are all contained in the subgroup generated by $y_\ell^{2^m}$. It follows in particular that $x_1^{2^m} = y_\ell^{k2^m}$, for some $k \geq 0$. If we let $x_1' = x_1 y_\ell^{-k}$ and $x_\ell' = x_\ell y_1^{-k}$, then $(x_1')^{2^m} = 1$ and the commuting relations are preserved. We may thus assume that $x_1^{2^m} = 1$. A similar argument for the other elements x_j, y_j, $1 \leq j \leq \ell-1$, show that we can assume that $x_j^{2^m} = y_j^{2^m} = 1$, for all $j = 1, \ldots, \ell-1$. In particular, the subgroup of P generated by these elements x_j, y_j, for $1 \leq j \leq \ell - 1$, is isomorphic to $X_{2(\ell-1)+1}(2^m)$.

If $x_\ell^{2^m}$ is contained in the subgroup generated by the element $(y_\ell^{2^m})^2$, then $x_\ell^{2^m} = (y_\ell^{2^{m+1}})^k$, for some $k \geq 0$. It follows from Lemma 1.4.20 that

$$(y_\ell^{-2k} x_\ell)^{2^m} = y_\ell^{-k2^{m+1}} x_\ell^{2^m} [y_\ell^{-2k}, x_\ell]^{2^{m-1}} = [y_\ell^{-2k}, x_\ell]^{2^{m-1}} = [y_\ell^{-k}, x_\ell]^{2^m} = 1.$$

Replacing, if needed, x_ℓ by $y_\ell^{-2k} x_\ell$, we may assume that $x_\ell^{2^m} = 1$. In this situation, the subgroup $\langle y_\ell, x_\ell\rangle$ is isomorphic to $M(m,s)$, where 2^s is the order of $y_\ell^{2^m}$.

Suppose finally that $y_\ell^{2^m}$ and $x_\ell^{2^m}$ generate the same subgroup of $Z(P)$. We may assume that $y_\ell^{2^m} = x_\ell^{2^m}$ and now

$$(y_\ell^{-1} x_\ell) = y_\ell^{-2^m} x_\ell^{2^m} [y_\ell^{-1}, x_\ell]^{2^{m-1}} = [y_\ell, x_\ell]^{2^{m-1}}.$$

Replacing x_ℓ by $y_\ell^{-1} x_\ell$, we may assume that $x_\ell^{2^m}$ has order 2. If $y_\ell^{2^m}$ has order strictly greater than 2, then we can apply the previous change on x_ℓ in order to have $x_\ell^{2^m} = 1$. If $y_\ell^{2^m}$ has order 2, then the subgroup $\langle y_\ell, x_\ell\rangle$ is isomorphic to the group $Q(m)$ and the proposition is proved. □

Remark 1.4.24. The more general classification of 2-groups of class 2 and cyclic center can be found in [9] and [19].

Chapter 2

Subgroup complexes

In this chapter, we give various results on upper intervals in the poset $\mathcal{A}_p(P)$ when P is a p-group. In Section 2.3, we determine exactly the homotopy type of $\mathcal{A}_p(P)_{\geq 2}$, when P is a p-group with a cyclic derived subgroup. We also determine for which of these groups, the poset $\mathcal{A}_p(P)$ is homotopically Cohen-Macaulay (see Section 2.5). We give in Section 2.4 a sharp upper bound, depending on the order of the group P, for the homological dimension of $\mathcal{A}_p(P)_{\geq 2}$. We give also a characterization of the groups for which this bound is reached. In Section 2.7, we derive, for any $Z \in \mathcal{A}_p(P)$, a spectral sequence E^1_{rs} converging to $\tilde{H}_{r+s}(\mathcal{A}_p(P))_{>Z}$. In Section 2.8, we give counterexamples to results of Fumagalli [12] and show some of their consequences.

2.1 Introduction

If G is a group, it is standard to denote by $\mathcal{S}_p(G)$ the partially ordered set (poset for short) of all non-trivial p-subgroups of G ordered by inclusion. This poset was introduced by Brown in [10]. Three years after Brown's paper, Quillen showed in [23] that the poset $\mathcal{S}_p(G)$ is homotopy equivalent to the poset $\mathcal{A}_p(G)$ of non-trivial elementary abelian p-subgroups of G, also ordered by inclusion. He began in this paper a systematic study of the topological properties of $\mathcal{A}_p(G)$. Despite the work of Quillen and others after him, there are still many questions concerning the homotopy type of $\mathcal{A}_p(G)$. A major one, attributed to Thévenaz by Pulkus and Welker in [22], is whether $\mathcal{A}_p(G)$ is homotopy equivalent to a wedge of spheres. A negative answer was given by Shareshian in [24], where he shows that $\tilde{H}_2(\mathcal{A}_3(S_{13}))$ is not torsion-free (note however that a part of this proof relies on computer calculations). In [12], Fumagalli claimed that the answer is positive if the group G is solvable. Unfortunately, his proof relies on a result that turns out to be false. We will come back to this later in Section 2.8. As a consequence, the following question seems to remain opened.

Question 2.1.1. If G is solvable, does $\mathcal{A}_p(G)$ have the homotopy type of a wedge of spheres ?

In [22], Pulkus and Welker showed that for solvable groups G the study of $\mathcal{A}_p(G)$ can be reduced to the study of upper intervals $\mathcal{A}_p(C_G(A))_{>A}$. According to [22], the homotopy type of these upper intervals is not clear, even for p-groups. A first result in this direction has been given by Bouc and Thévenaz in [8], where they study the poset $\mathcal{A}_p(P)_{\geq 2}$ of all elementary abelian subgroups of P of rank at least 2. They show that for any p-group P, the poset $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of spheres. It is related to upper intervals by the following: For $A \in \mathcal{A}_p(P)$ with $|A| = p$ there is a homotopy equivalence $\mathcal{A}_p(P)_{\geq 2} \simeq \mathcal{A}_p(C_P(A))_{\geq 2}$ (see Lemma 2.3.1 and Lemma 2.3.3). Knowing that $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of spheres, one can ask more precise questions on the dimension of these spheres. Computer calculations led Bouc and Thévenaz to raise the following questions.

Question 2.1.2 (Bouc, Thévenaz)**.** Let P be a p-group. Do the spheres occurring in $\mathcal{A}_p(P)_{\geq 2}$ all have the same dimension if p is odd ? Does one get only two consecutive dimensions if $p = 2$?

In Section 2.3 we will show that p-groups with a cyclic derived subgroup give a partial answer to this question. For this, we will use a result of Bouc and Thévenaz that allows recursive computations of the homotopy type of posets of the form $\mathcal{A}_p(P)_{\geq 2}$. Of course, the dimension of the spheres occurring in $\mathcal{A}_p(P)_{\geq 2}$ is at most the dimension of the complex $\mathcal{A}_p(P)_{\geq 2}$, that is, $\mathrm{rk}(P) - 2$. In Section 2.4 we will give a sharper bound, depending on the order of the group. We will show that there are p-groups for which this bound is reached and we will also give some information on these p-groups.

The structure of upper intervals in $\mathcal{A}_p(G)$ is also important to determine whether the poset $\mathcal{A}_p(G)$ is homotopy Cohen-Macaulay (hCM for short). Recall that a poset $\mathcal{P}$ is hCM if it is spherical of dimension $d = \dim \mathcal{P}$ and the link of each k simplex in $\mathcal{P}$ is $(d-k-1)$-spherical. For the poset $\mathcal{A}_p(G)$ it is equivalent to require that $\mathcal{A}_p(G)$ is spherical of dimension $r_p(G) - 1$ and for any $B \in \mathcal{A}_p(G)$ the poset $\mathcal{A}_p(G)_{>B}$ is spherical of dimension $r_p(G) - r_p(B) - 1$ (see [23, Proposition 10.1]).

In Section 2.5, we will determine for which of the p-groups with cyclic derived subgroup the poset $\mathcal{A}_p(P)$ is hCM. Thanks to work of Quillen these informations can be lifted to p-nilpotent groups. More precisely, Quillen has shown for a p-nilpotent group G with $P = G/O_{p'}(G)$ that $\mathcal{A}_p(G)$ is hCM if $\mathcal{A}_p(P)$ is.

In Section 2.7, we will try to generalize the work of Bouc and Thévenaz for upper intervals $\mathcal{A}_p(P)_{>A}$, when A has rank at least 2. Their method can be generalized but only for very particular cases. To tackle the problem in general, we make use of a spectral sequence introduced by Quillen in [23]. For a poset map $f : \mathcal{P} \to \mathcal{Q}$, this spectral sequence has the following form:

$$E^2_{rs} = H_r\left(\mathcal{Q}, q \mapsto H_s(f^{-1}_{\leq q})\right) \Rightarrow H_{r+s}(\mathcal{P})$$

As the notation $q \mapsto H_s(f^{-1}_{\leq q})$ suggests, the homology groups occurring in the E^2-page of the spectral sequence are not usual homology groups with a constant abelian group as coefficients. Before going on with the applications of this spectral sequence, we recall in Section 2.6 the definition of homology with non-constant coefficients and we derive a spectral sequence given in term of standard homology groups converging to homology groups with non-constant coefficients. We apply these results in Section 2.7 and derive another spectral sequence converging to the homology groups of $\mathcal{A}_p(P)_{>A}$. However, this spectral sequence doesn't seem to be very convenient for calculations or to obtain general results.

In Section 2.8, we will come back to Fumagalli's claim that $\mathcal{A}_p(G)$ has the homotopy type of a wedge of spheres when G is solvable. We will exhibit counterexamples to a fiber theorem [12, Corollary 5] on which the proof of his general result relies. We will also show how this affects the rest of his paper.

2.2 Preliminaries on posets

We recall here some definitions and notation in the topic of partially ordered sets (*posets* for short). All posets are supposed to be finite. The reader can refer to Quillen's paper [23] or to Wachs' survey on topology of posets [30] for more details.

We will mostly use script letters like $\mathcal{P}$ or $\mathcal{Q}$ to denote an arbitrary poset. For a poset $\mathcal{P}$, we will use the same letter to denote its *order complex*, that is the (abstract) simplicial complex whose vertices are the elements of $\mathcal{P}$ and whose faces are the chains of elements of $\mathcal{P}$. The order complex of $\mathcal{P}$ has a geometric realization, that we still denote $\mathcal{P}$, which is in particular a topological space. If we say that a poset $\mathcal{P}$ has a certain topological property, we mean that the geometric realization of the order complex of $\mathcal{P}$ has this property.

Recall that a poset is *bounded* if it has a unique maximum element, called the *top element*, and a unique minimum element, called the *bottom element*. The top element is usually denoted by $\hat{1}$ and the bottom element by $\hat{0}$. If $\mathcal{P}$ is a poset, one can add a bottom element $\hat{0}$ and a top element $\hat{1}$ to $\mathcal{P}$ and define the *bounded extension* $\hat{\mathcal{P}} = \mathcal{P} \cup \{\hat{0}, \hat{1}\}$.

We will say that $\mathcal{P}$ is a *discrete poset* if the (partial) order on $\mathcal{P}$ is given by the identity, i.e. for $x, x' \in \mathcal{P}$, one has $x \leq x'$ if and only if $x = x'$. There is thus no order relation between two distinct elements of $\mathcal{P}$ and the geometric realization of $\mathcal{P}$ is a disjoint union of points, hence has the homotopy type of a wedge of spheres of dimension 0.

Height, intervals and rank

For an element x of a poset $\mathcal{P}$ we denote by $\mathcal{P}_{\leq x}$ the subposet of $\mathcal{P}$ defined by

$$\mathcal{P}_{\leq x} = \{x' \in \mathcal{P} \,|\, x' \leq x\}.$$

We also define $\mathcal{P}_{<x}$ as the subposet

$$\mathcal{P}_{<p} = \{x' \in \mathcal{P} \,|\, x' < x\}.$$

The posets $\mathcal{P}_{\geq x}$ and $\mathcal{P}_{>x}$ are defined similarly. For $x_1 < x_2$, the closed interval $[x_1, x_2]$ is the poset $\mathcal{P}_{\geq x_1} \cap \mathcal{P}_{\leq x_2}$ and the open interval (x_1, x_2) is $\mathcal{P}_{>x_1} \cap \mathcal{P}_{<x_2}$.

A *k-chain* of a poset $\mathcal{P}$ is a totally ordered subset $c = \{x_0 < x_1 < \cdots < x_k\}$ of $\mathcal{P}$. The integer k is called the *length* of the chain c and is denoted by $l(c)$. We make the convention that the empty set is a chain of dimension -1. We also define $l(\mathcal{P})$ to be the maximum of $\{l(c) \,|\, c \text{ is a chain of } \mathcal{P}\}$. Since $l(\mathcal{P})$ is equal to the dimension of the order complex of $\mathcal{P}$ we will frequently call $l(\mathcal{P})$ the dimension of $\mathcal{P}$.

For an element x of a poset $\mathcal{P}$, we denote by $h_{\mathcal{P}}(x)$ the *height* of x in $\mathcal{P}$ defined by $h_{\mathcal{P}}(x) = l(\mathcal{P}_{\leq x})$. If the poset $\mathcal{P}$ is clear in the context, we will sometimes omit the subscript and write simply $h(x)$ instead of $h_{\mathcal{P}}(x)$.

If $\mathcal{P}$ is a bounded poset, we define the *rank* of $x \in \mathcal{P}$ by $r(x) = l([\hat{0}, x])$. For a subset $R \subseteq \{0, \ldots, l(\mathcal{P}) - 1\}$, we define the *rank-selected* subposet

$$\mathcal{P}_R = \{x \in \mathcal{P} \mid r(x) \in R\}.$$

We will denote by $\mathcal{P}_{\geq r}$ the rank-selected poset corresponding to $[r, \ldots, l(P)-1]$, that is

$$\mathcal{P}_{\geq r} = \{x \in \mathcal{P} \mid r(x) \geq r\}.$$

Poset maps and fibers

Let $\mathcal{P}$ and $\mathcal{Q}$ be posets. A poset map $f : \mathcal{P} \to \mathcal{Q}$ is an order-preserving map, that is, $f(x) \leq f(x')$ if $x \leq x'$.

Definition 2.2.1. If $f : \mathcal{P} \to \mathcal{Q}$ is a poset map, the fiber above an element $q \in \mathcal{Q}$ is the subposet of $\mathcal{P}$ defined by

$$f^{-1}_{\leq q} = \{x \in \mathcal{P} \mid f(x) \leq q\}.$$

Recall that a poset $f : \mathcal{P} \to \mathcal{Q}$ induces a natural map between the geometric realization of $\mathcal{P}$ and $\mathcal{Q}$.

Lemma 2.2.2. *If $f, g : \mathcal{P} \to \mathcal{Q}$ are poset maps such that $f(x) \leq g(x)$ for all $x \in \mathcal{P}$, then the induced maps are homotopic.*

Proof. See 1.3 in Quillen's paper [23]. □

The following lemma, due to Quillen, has proved especially useful in the study of topology of posets and is often referred to as the "Quillen fiber lemma".

Lemma 2.2.3 ("Quillen fiber lemma")**.** *If $f : \mathcal{P} \to \mathcal{Q}$ is a poset map such that $f^{-1}_{\leq q}$ is contractible for all $q \in \mathcal{Q}$, then f is a homotopy equivalence.*

Proof. See [23] or [29]. □

Contractibility, sphericity and hCM property

Definition 2.2.4. A poset $\mathcal{P}$ is conically contractible if there is a poset map $f : \mathcal{P} \to \mathcal{P}$ and an element $x_0 \in \mathcal{P}$ such that

$$x \leq f(x) \geq x_0, \qquad \text{for all } x \in \mathcal{P}.$$

Recall that for two elements x, y of a poset $\mathcal{P}$, the *join* $x \vee y$ of x and y in $\mathcal{P}$ is an element of $\mathcal{P}$ greater than or equal to both x and y that is less than all other such elements. This element $x \vee y$ may not exist, but if it exists it is unique.

Definition 2.2.5. An element $x_0 \in \mathcal{P}$ is a conjunctive element if for each $x \in \mathcal{P}$ the join $x \vee x_0$ exists in $\mathcal{P}$.

The following result follows from Lemma 2.2.2 and the fact that the geometric realization of a poset with a top element is a cone, hence is contractible.

Lemma 2.2.6. *If a poset $\mathcal{P}$ is conically contractible or has a conjunctive element, then $\mathcal{P}$ is contractible.*

Definition 2.2.7. A poset $\mathcal{P}$ is k-spherical, or spherical of dimension k, if it has the homotopy type of a wedge of spheres of dimension k. The poset $\mathcal{P}$ is spherical of maximal dimension if it is $\dim \mathcal{P}$-spherical.

Remark 2.2.8. Note that in our definition of a k-spherical poset, we don't require k to be equal to the dimension of the poset.

Definition 2.2.9. Let $\mathcal{P}$ be a poset with bounded extension $\hat{\mathcal{P}} := \mathcal{P} \cup \{0, 1\}$. The poset $\mathcal{P}$ is homotopically Cohen-Macaulay, hCM for short, if for all $x' < x$ in $\hat{\mathcal{P}}$ the interval (x', x) is homotopy equivalent to a wedge of spheres of dimension $h(x) - h(x') - 2$.

Remark 2.2.10. The height of an element x of $\mathcal{P}$ is different, depending on whether x is considered as an element in $\mathcal{P}$ or $\hat{\mathcal{P}}$. Because of the presence of the bottom element, the height of x in $\mathcal{P}$ is one less that its height in $\hat{\mathcal{P}}$. However, the dimension of the open intervals in the previous definition, namely $h(x') - h(x) - 2$ is the same in $\mathcal{P}$ and $\hat{\mathcal{P}}$.

Proposition 2.2.11 (Corollary 9.7 in [23])**.** *Let $f : \mathcal{P} \to \mathcal{Q}$ be a strictly increasing poset map, that is $x' < x$ implies $f(x') < f(x)$. If $\mathcal{Q}$ is hCM of dimension d and $f^{-1}_{\leq q}$ is hCM of dimension $h(q)$ for all $q \in \mathcal{Q}$, then $\mathcal{P}$ is hCM of dimension d.*

Homology

For any poset $\mathcal{P}$ and any integer $k \geq -1$, the reduced chain space $\tilde{C}_k(\mathcal{P})$ is the free abelian group generated by the k-chains of P. Note that since we consider the empty set as a chain of dimension -1, we have $C_{-1}(\mathcal{P}) = \mathbb{Z}$. We set $\tilde{C}_{-2}(\mathcal{P}) = 0$ and for $k \geq -1$, the boundary map $\partial_k : \tilde{C}_k(\mathcal{P}) \to \tilde{C}_{k-1}(\mathcal{P})$ is defined by

$$\partial_k(x_0 < \cdots < x_k) = \sum_{i=0}^{k} (-1)^i (x_0 < \cdots < \hat{x}_i < \cdots < x_k),$$

where $\hat{\cdot}$ denotes deletion. We have $\partial_{k-1}\partial_k = 0$ and the *reduced homology groups* $\tilde{H}_k(\mathcal{P})$ of $\mathcal{P}$ are defined as the homology groups of the complex $(\tilde{C}_k(\mathcal{P}), \partial_k)$.

Remark 2.2.12. Note that one has in particular

$$\tilde{H}_k(\emptyset) = \begin{cases} \mathbb{Z} & \text{if } k = -1. \\ 0 & \text{else.} \end{cases}$$

If $\mathcal{P}$ is not empty, then $\tilde{H}_{-1}(\mathcal{P}) = 0$.

The *(non-reduced) homology groups* $H_k(\mathcal{P})$ of $\mathcal{P}$ are defined as the homology groups of the complex $(C_k(\mathcal{P}), \partial_k)$, where $C_{-1}(\mathcal{P}) = 0$ and $C_k(\mathcal{P}) = \tilde{C}_k(\mathcal{P})$ for $k \geq 0$. The boundary map is defined as above.

Remark 2.2.13. For $k \geq 1$, one has $H_k(\mathcal{P}) = \tilde{H}_k(\mathcal{P})$.

Definition 2.2.14. The suspension of a poset $\mathcal{P}$ is the poset $\Sigma\mathcal{P} = \mathcal{P} \cup \{o_1, o_2\}$, where o_1 and o_2 are smaller than every element of $\mathcal{P}$ but there is no order relation between o_1 and o_2.

Remark 2.2.15. In the particular case $\mathcal{P} = \emptyset$, one has that $\Sigma\emptyset$ is is a discrete poset consisting of two points.

The geometric realization of $\Sigma\mathcal{P}$ is the usual suspension of the geometric realization of $\mathcal{P}$. One has in particular the following lemma.

Lemma 2.2.16. *For $k \geq 0$, there is an isomorphism $\tilde{H}_k(\Sigma\mathcal{P}) \cong \tilde{H}_{k-1}(\mathcal{P})$.*

2.3 The poset $\mathcal{A}_p(P)_{\geq 2}$

Introduction

We begin this section by recalling two general elementary facts.

Lemma 2.3.1. *If P is a p-group, then*

a) $\mathcal{A}_p(P) = \mathcal{A}_p(\Omega_1(P))$,

b) $\mathcal{A}_p(P)_{>A} = \mathcal{A}_p(C_P(A))_{>A}$ for any $A \in \mathcal{A}_p(P)$.

Proof. Part a) follows from the fact that any $B \in \mathcal{A}_p(P)$ has exponent p and part b) comes from the fact that any $B \in \mathcal{A}_p(P)_{>A}$ centralizes A. ☐

Remark 2.3.2. Part a) of the previous lemma allows one to make the assumption that P is generated by elements of order p. Part b) allows one to make the assumption that A is central in P.

The following lemma shows the relation between upper intervals and rank-selected posets in $\mathcal{A}_p(P)$.

Lemma 2.3.3. *Let P be a p-group and $A \in \mathcal{A}_p(P)$. If A is central in P, the inclusion $\mathcal{A}_p(P)_{>A} \hookrightarrow \mathcal{A}_p(P)_{\geq \mathrm{rk}(A)+1}$ is a homotopy equivalence.*

Proof. The homotopy inverse is the map $\mathcal{A}_p(P)_{\geq \mathrm{rk}(A)+1} \to \mathcal{A}_p(P)_{>A}$ given by $B \mapsto BA$ for all $B \in \mathcal{A}_p(P)_{\geq \mathrm{rk}(A)+1}$. ☐

Remark 2.3.4. This lemma shows that upper intervals can always be seen as rank-selected posets, but the converse is not true in general. Consider for example the poset $\mathcal{A}_p(P)_{\geq 3}$ for $P = X_{p^5}$. Since P has rank 3, the poset $\mathcal{A}_p(P)_{\geq 3}$ is the discrete poset consisting of all elementary abelian subgroups of rank 3. If $A \in \mathcal{A}_p(P)$ has rank 3, then $\mathcal{A}_p(P)_{>A}$ is empty. If A does not contain $Z(P)$ then $\mathcal{A}_p(P)_{>A}$ is conically contractible via $B \leq BZ(P) \geq AZ(P)$. If A

contains $Z(P)$ and has rank 2, then $\mathcal{A}_p(P)_{>A}$ is the discrete poset of all elementary abelian subgroups of rank 3 containing A. It is not difficult to see that the number of points in $\mathcal{A}_p(P)_{\geq 3}$ and $\mathcal{A}_p(P)_{>A}$ is different, so that they are not homotopy equivalent. We will see later in this section that $\mathcal{A}_p(P)_{>Z(P)}$ is a (non-empty) wedge of spheres of dimension 1, hence cannot be homotopy equivalent to $\mathcal{A}_p(P)_{\geq 3}$. All this shows that the subposet $\mathcal{A}_p(P)_{\geq 3}$ is not homotopy equivalent to any of the upper intervals of $\mathcal{A}_p(P)$.

Remark 2.3.5. If A has order p and A is central in P, then the previous lemma shows that the two posets $\mathcal{A}_p(P)_{>A}$ and $\mathcal{A}_p(P)_{\geq 2}$ are homotopy equivalent. We will alternatively consider one or the other depending on which is more convenient and we may sometimes pass from one to the other without any warning.

The posets of the form $\mathcal{A}_p(P)_{\geq 2}$ have been studied by Bouc and Thévenaz in [8]. They have shown in particular a wedge decomposition formula that allows recursive calculations. As a corollary, they obtain that for any p-group P the poset $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of spheres.

In this section, we will use this formula to compute explicitly the homotopy type of $\mathcal{A}_p(P)_{\geq 2}$ for all p-groups with cyclic derived subgroup. The results of these calculations can be found in Table 2.1 on page 74.

The Bouc-Thévenaz Wedge Decomposition Formula

The following proposition is a slight generalization of the original result of Bouc and Thévenaz concerning $\mathcal{A}_p(P)_{\geq 2}$. We present here a very similar but somewhat shorter proof using a homotopy complementation formula that we state first.

Lemma 2.3.6 (Homotopy complementation formula)**.** *Let $\mathcal{P}$ be a poset and let $\mathcal{M}$ be a subset of $\mathcal{P}$ consisting of minimal elements of $\mathcal{P}$. If the poset $\overline{\mathcal{P}} = \mathcal{P} - \mathcal{M}$ is contractible, then*

$$\mathcal{P} \simeq \bigvee_{x \in \mathcal{M}} \Sigma \operatorname{lk}_{\overline{\mathcal{P}}}(x).$$

Proof. See for example Corollary 2.3 in [6]. $\square$

Proposition 2.3.7. *Let Z be a central elementary abelian subgroup of a p-group P. Suppose that P contains a normal subgroup $E_0 \in \mathcal{A}_p(P)_{>Z}$ with $|E_0 : Z| = p$ and such that $M := C_P(E_0)$ has index p in P. Then,*

$$\mathcal{A}_p(P)_{>Z} \simeq \bigvee_{F \in \mathcal{F}} \Sigma \mathcal{A}_p(C_M(F))_{>Z}, \tag{2.1}$$

where $\mathcal{F} = \{F \in \mathcal{A}_p(P)_{>Z} \,|\, F \cap M = Z\}$.

Proof. Let $\mathcal{T}$ be the poset $\mathcal{A}_p(P)_{>Z} - \mathcal{F}$ and $B \in \mathcal{T}$. Since $B \notin \mathcal{F}$, we have $B \cap M > Z$ and the following sequence of inequalities in $\mathcal{T}$ shows that the poset $\mathcal{T}$ is contractible:

$$B \geq B \cap M \leq (B \cap M)E_0 \geq E_0.$$

Since $|P : M| = p$, we have $|B : B \cap M| = p$, so that $B \cap M > Z$ if $\mathrm{rk}(B/Z) \geq 2$. It follows that the set $\mathcal{F}$ consists of minimal elements of $\mathcal{A}_p(P)_{>Z}$.

It follows now from the homotopy complementation formula that there is a homotopy equivalence

$$\mathcal{A}_p(P)_{>Z} \simeq \bigvee_{F \in \mathcal{F}} \Sigma \, \mathrm{lk}_{\mathcal{T}}(F).$$

Furthermore, $\mathrm{lk}_{\mathcal{T}}(F) = \mathcal{A}_p(P)_{>F}$, so that it remains to show that $\mathcal{A}_p(P)_{>F}$ is homotopy equivalent to $\mathcal{A}_p(C_M(F))_{>Z}$.

Remark that for $B \in \mathcal{A}_p(P)_{>F}$, we have $B \cap M > Z$ since $|P : M| = p$ and $B \cap M \leq B$ centralizes F. It follows that we can then define a poset map $g : \mathcal{A}_p(P)_{>F} \to \mathcal{A}_p(C_M(F))_{>Z}$ by $g(B) = B \cap M$. On the other hand, we have $F \cap M = Z$, so that $EF > F$ for any $E \in \mathcal{A}_p(P)_{>F}$. We can thus define a poset map $q : \mathcal{A}_p(C_M(F))_{>Z} \to \mathcal{A}_p(P)_{>F}$ by $q(E) = EF$.

For any $B \in \mathcal{A}_p(P)_{>F}$, we have $qg(B) = q(B \cap M) = (B \cap M)F \leq B$ and for any $E \in \mathcal{A}_p(C_M(F))_{>Z}$, we have $gq(E) = (EF) \cap M \geq E$. It follows now from Lemma 2.2.2 that $\mathcal{A}_p(P)_{>F}$ is homotopy equivalent to $\mathcal{A}_p(C_M(F))_{>Z}$. □

The main difficulty is that such a subgroup E_0 with these properties may not exist. If Z is not maximal in $\mathcal{A}_p(P)$, then the next lemma shows that, at least when p is odd, one of the elementary abelian subgroups covering Z is normal in P. The problem here is that the index of the centralizer of E in P may be strictly greater than p.

Lemma 2.3.8 (Hobby)**.** *Let p be an odd prime and let Z be an elementary abelian subgroup of a p-group P. If Z is normal in P and Z is not maximal among elementary abelian subgroups of P, then there exists a normal elementary abelian subgroup E of P such that $|E : Z| = p$.*

Proof. See Lemma 1 in [17]. □

When A has order p, we obtain the original result of Bouc and Thévenaz as a corollary of Proposition 2.3.7.

Corollary 2.3.9 (Bouc, Thévenaz)**.** *Let P be a p-group with cyclic center and let $Z = \Omega_1(Z(P))$. Suppose that P contains a normal elementary abelian subgroup E_0 of rank 2. Then*

$$\mathcal{A}_p(P)_{\geq 2} \simeq \bigvee_{F \in \mathcal{F}} \Sigma \mathcal{A}_p(C_M(F))_{\geq 2}, \tag{2.2}$$

where $\mathcal{F} = \{F \in \mathcal{A}_p(P)_{>Z} \,|\, M \cap F = Z\}$.

Proof. Since $Z(P)$ is cyclic, the subgroup $Z = \Omega_1(Z(P))$ has order p. The normal subgroup E_0 contains Z and considering the action of P on E_0 by conjugation, one sees that $|P : C_P(E_0)| = p$. The result follows now directly from Proposition 2.3.7. □

Remark 2.3.10. We will refer to corollary 2.3.9 as the Bouc-Thévenaz Wedge Decomposition Formula and we will also refer to Proposition 2.3.7 as the generalized Bouc-Thévenaz Wedge Decomposition Formula.

The following is a homological version of the Bouc-Thévenaz Wedge Decomposition Formula.

Corollary 2.3.11. *Let P be a p-group with cyclic center and let $Z = \Omega_1(Z(P))$. Suppose that P contains a normal elementary abelian subgroup E_0 of rank 2. Then for each $k \geq 0$*

$$\tilde{H}_k(\mathcal{A}_p(P)_{\geq 2}) \cong \bigoplus_{F \in \mathcal{F}} \tilde{H}_{k-1}(\mathcal{A}_p(C_M(F))_{\geq 2}), \tag{2.3}$$

where $\mathcal{F} = \{F \in \mathcal{A}_p(P)_{\geq 2} \,\big|\, M \cap F = Z\}$.

Lemma 2.3.12. *If P is a p-group with no noncyclic abelian normal subgroups, then either P is cyclic, or $p = 2$ and P is isomorphic to $D_{2^{m+2}}$, $m > 1$, $Q_{2^{m+2}}$, $m \geq 1$, or $SD_{2^{m+2}}$, $m > 1$.*

Proof. See for example Theorem 5.4.10 in [14]. □

The proof of the following result is due to Bouc and Thévenaz [8]. We have included their proof for sake of completeness.

Proposition 2.3.13 (Bouc, Thévenaz)**.** *For any p-group P, the poset $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of spheres.*

Proof. If the center of P is not cyclic, then $\Omega_1(Z(P))$ is a conjunctive element in the poset $\mathcal{A}_p(P)_{\geq 2}$ which is then contractible. Otherwise, if P does not contain a normal elementary abelian subgroup of rank 2, then P is one of the groups given in Lemma 2.3.12. For these particular groups, the poset $\mathcal{A}_p(P)_{\geq 2}$ is easily seen to be homotopy equivalent to a wedge of spheres. The result follows now from a recursive use of Corollary 2.3.9. □

Computations for p-groups with a cyclic derived subgroup

What follows is a partial answer to Question 2.1.2 concerning the dimension of spheres occurring in the homotopy type of $\mathcal{A}_p(P)_{\geq 2}$. We will show that p-groups with cyclic derived subgroup give a partial positive answer to this question.

As a first step, we can make the following reductions. Let P be a p-group with cyclic derived subgroup. If $Z(P)$ is not cyclic, then $\Omega_1(Z(P))$ is a conjunctive element in $\mathcal{A}_p(P)_{\geq 2}$, so that $\mathcal{A}_p(P)_{\geq 2}$ is contractible. Recall that we may also suppose $P = \Omega_1(P)$, that is, P is generated by elements of order p. But then P/P' is also generated by elements of order p, hence must be elementary abelian. It follows that $P' = \Phi(P)$, hence we may assume that $\Phi(P)$ is cyclic.

We can thus restrict our attention to p-groups generated by elements of order p such that $\Phi(P)$ and $Z(P)$ are cyclic. When p is odd, Theorem 1.3.26 implies that these assumptions are only satisfied if P is extraspecial of type I. We will treat this case as a first example.

Example 2.3.14. Let p be an odd prime and suppose that $P = X_{p^{2\ell+1}}$ is extraspecial of type I. For such a group, the homotopy type of $\mathcal{A}_p(P)_{>Z(P)} \simeq \mathcal{A}_p(P)_{\geq 2}$ has been determined by Quillen [23] and his argument goes as follows.

Recall that $P/Z(P)$ is endowed with a non-degenerate alternating form induced by commutators. It follows by the definition of the alternating form that a subgroup H of P strictly containing $Z(P)$ is abelian if and only if the corresponding subspace H/Z is non-trivial totally isotropic. Since P has exponent p, the poset $\mathcal{A}_p(P)_{>Z(P)}$ is thus isomorphic to the poset of non-trivial totally isotropic subspaces in $P/Z(P)$. This poset in turn is homotopy equivalent to the building of a symplectic group. The Solomon-Tits theorem implies now that $\mathcal{A}_p(P)_{>Z(P)}$ has the homotopy type of a wedge of spheres p^{ℓ^2} spheres of dimension $\ell - 1$.

The result of the preceding example is stated in the following lemma. We would like however to give an alternative proof of it using the Bouc-Thévenaz Wedge Decomposition Formula. This proof will serve as a prototype for all other computations in this section.

Lemma 2.3.15. *Let p be an odd prime. If $P = X_{p^{2\ell+1}}$ with $\ell \geq 1$, then $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of p^{ℓ^2} spheres of dimension $\ell - 1$.*

Proof. Suppose first that $\ell = 1$, so that $P = X_{p^3}$. In this situation, $\mathcal{A}_p(P)_{>Z(P)}$ is isomorphic to the poset of all non-trivial proper subspaces of $P/Z(P)$. It follows at once that $\mathcal{A}_p(P)_{>Z(P)}$ is a discrete poset consisting of $p+1$ points, hence has the homotopy type of a wedge of p spheres of dimension 0.

Suppose now $\ell > 1$ and let z be a generator of $Z(P)$. Recall that we can choose symplectic generators $x_1, y_1, \ldots, x_\ell, y_\ell$ of P such that $[x_i, y_i] = z$ and $x_i^p = y_i^p = 1$ for all $i = 1, \ldots, \ell$. Let E_0 be the elementary abelian subgroup of rank 2 generated by z and y_1. Then E_0 is normal in P (it contains P') and $M = C_P(E_0)$ is generated by E_0 and all other generators except x_1, that is

$$M = \langle z, y_1, x_2, y_2, \ldots, x_\ell, y_\ell \rangle.$$

The Bouc-Thévenaz Wedge Decomposition Formula gives then

$$\mathcal{A}_p(P)_{>Z(P)} \simeq \bigvee_{F \in \mathcal{F}} \Sigma \mathcal{A}_p(C_M(F))_{>Z(P)}, \tag{2.4}$$

where $\mathcal{F} = \{F \in \mathcal{A}_p(P)_{>Z(P)} \,\big|\, F \cap M = Z(P)\}$. Remark that $\mathcal{F}$ corresponds bijectively to the set of all 1-dimensional complements of $M/Z(P)$ in $P/Z(P)$, so that $|\mathcal{F}| = p^{2\ell-1}$. A subgroup $F \in \mathcal{F}$ is generated by z and an element of the form $x_1 y_1^k x$ with $0 \leq k < p$ and $x \in \langle x_2, y_2, \ldots, x_\ell, y_\ell \rangle$. Without any loss of generality, we may assume $x = x_2$.

We claim that $C_M(F)$ is extraspecial of type I and order $p^{2(\ell-1)+1}$. To see this, we show that $C_M(F)$ is equal to the subgroup K of P defined by

$$K = \langle x_2, y_1^{-1} y_2, x_3, y_3, \ldots, x_\ell, y_\ell \rangle.$$

Except possibly for $y_2 y_1^{-1}$, it is clear that these elements are in $C_M(F)$. But since the commutators are central, we also have

$$[x_1 y_1^k x_2, y_2 y_1^{-1}] = [x_1, y_1]^{-1} [x_2, y_2] = z^{-1} z = 1.$$

Furthermore, the subgroup generated by x_2 and $y_1^{-1}y_2$ is isomorphic to X_{p^3} since y_1 commutes with both x_2 and y_2. It follows then that K is extraspecial of type I and order $p^{2(\ell-1)+1}$.

Since F is a normal elementary abelian subgroup of P of rank 2, we have $|P : C_P(F)| = p$. Furthermore, $|P : M| = p$ and $C_p(F) \neq M$ since $y_1 \in M$ but $y_1 \notin C_P(F)$. It follows that $C_M(F) = C_P(F) \cap M$ has index p in M, hence has index p^2 in P. Therefore, $C_M(F)$ has order $p^{2\ell-1}$ and this shows that K and $C_M(F)$ have the same order, hence $K = C_M(F)$.

By a recursive argument we have now for any $F \in \mathcal{F}$ that $\mathcal{A}_p(C_M(F))_{>Z(P)}$ has the homotopy type of a wedge of $p^{(\ell-1)^2}$ spheres of dimension $\ell-2$. Putting this information in equation (2.4), we see that $\mathcal{A}_p(P)_{>Z(P)}$ has the homotopy type of $p^{2\ell-1}\cdot p^{(\ell-1)^2} = p^{\ell^2}$ spheres of dimension $\ell-1$ (the dimension is increased by the suspension) and the lemma is proved. □

The following proposition follows now immediately from the previous lemma and the reductions made before. Note that this result closes the discussion for p odd.

Proposition 2.3.16. *Let p be an odd prime. If P is a p-group with a cyclic derived subgroup, then $\mathcal{A}_p(P)_{\geq 2}$ is contractible, unless $\Omega_1(P)$ is extraspecial of type I, say $\Omega_1(P) = X_{p^{2\ell+1}}$, in which case $\mathcal{A}_p(P)_{\geq 2}$ is homotopy equivalent to a wedge of p^{ℓ^2} spheres of dimension $\ell - 1$.*

When $p = 2$ the situation is more complicated. However, in similarity with the case p odd, an argument using buildings and the Solomon-Tits theorem can be used when $\Phi(P)$ has order 2. As for p odd, we will give a proof avoiding buildings and based on the Bouc-Thévenaz Wedge Decomposition Formula. The proofs are similar to the case p odd, but we have to be more careful with the order of the elements.

Lemma 2.3.17.

a) If $P = D_8^{*\ell}$ with $\ell \geq 1$, then $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of $2^{\ell(\ell-1)}$ spheres of dimension $\ell - 1$.

b) If $P = D_8^{*\ell} * C_4$ with $\ell \geq 0$, then $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of 2^{ℓ^2} spheres of dimension $\ell - 1$.

c) If $P = D_8^{*\ell} * Q_8$ with $\ell \geq 0$, then $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of $2^{\ell(\ell+1)}$ spheres of dimension $\ell - 1$.

Proof.

a) If $P = D_8$, then $\mathcal{A}_p(P)_{>Z(P)}$ is easily seen to consist of 2 points, hence $\mathcal{A}_p(P)_{>Z(P)}$ has the homotopy type of a sphere of dimension 0. Suppose now that $P = D_8^{*\ell}$ with $\ell > 1$. Let z be a generator of $Z(P)$ and let $x_1, y_1, \ldots, x_\ell, y_\ell$ be symplectic generators of P all of order 2 and such that $[x_i, y_i] = z$. Let E_0 be the elementary abelian subgroup of P of rank 2 generated by z and y_1. It is clear that E_0 is normal in P and $M = C_P(E_0)$ is generated by E_0 and all other generators of P except x_1, that is

$$M = \langle z, y_1, x_2, y_2, \ldots, x_\ell, y_\ell \rangle.$$

The Bouc-Thévenaz Wedge Decomposition Formula gives then

$$\mathcal{A}_p(P)_{>Z(P)} \simeq \bigvee_{F\in\mathcal{F}} \Sigma\mathcal{A}_p(C_M(F))_{>Z(P)}, \tag{2.5}$$

where $\mathcal{F} = \{F \in \mathcal{A}_p(P)_{>Z(P)} \,|\, F\cap M = Z(P)\}$. A subgroup $F \in \mathcal{F}$ is generated by z and an element $x_1y_1^kx$ with $k\in\{0,1\}$ and x is in the subgroup D generated by the x_j, y_j for $j = 2,\dots,\ell$. Note that this subgroup D is isomorphic to $D_8^{*(\ell-1)}$. Since $F\in\mathcal{F}$ is elementary abelian, we must have

$$1 = (x_1y_1^kx)^2 = z^kx^2.$$

We have therefore $k = 0$ if $x^2 = 1$ and we have $k = 1$ if $x^2 = z$. Any element $x \in D$ defines thus a subgroup $F(x)$ in $\mathcal{F}$ by $F(x) = \langle z, x_1y_1^kx\rangle$ where k is chosen such that $k = 1$ if $x^2 = z$ and $k = 0$ otherwise. Furthermore, two elements of D define the same subgroup in $\mathcal{F}$ if and only if they differ by an element of $Z(P)$. The subgroups in $\mathcal{F}$ correspond then bijectively with $D/Z(D)$, hence $\mathcal{F}$ has cardinality $2^{2(\ell-1)}$.

If $F = \langle z, x_1y_1^kx\rangle \in \mathcal{F}$, then we claim that $C_M(F)$ is isomorphic to $D_8^{*(\ell-1)}$. Suppose first that $k = 0$. Without loss of generality we may assume that $x = x_2$ or $x = 1$. In this case, the centralizer of F in M is easily seen to be generated by x_2, y_1y_2, respectively x_2, y_2 if $x = 1$, and the elements x_j, y_j for $3 \le j \le \ell$. It follows that $C_M(F)$ is isomorphic to $D_8^{*(\ell-1)}$.

If $k = 1$, we may suppose without loss of generality that $x = x_2y_2$. In this case, the centralizer of F in M is generated by x_2y_2, y_2y_1 and the elements x_j, y_j for $3 \le j \le \ell$. In this case also $C_M(F)$ is isomorphic to $D_8^{*(\ell-1)}$ and our claim is proved.

We have then that $\mathcal{A}_p(D_8^{*\ell})_{\ge 2}$ has the homotopy type of a wedge of $2^{2(\ell-1)}$ copies of the suspension of $\mathcal{A}_p(D_8^{*(\ell-1)})_{\ge 2}$. The result follows now by an induction argument.

b) Let $P = D_8 * C_4$. A close look at the elements of order 2 in P shows that $\mathcal{A}_p(P)_{>Z(P)}$ consists of three isolated points, hence has the homotopy type of a wedge of 2 spheres of dimension 0. Suppose now $\ell > 1$ and $P = D_8^{*\ell} * C_4$. Let c be a generator of $Z(P)$ and let $z = c^2$. We can choose symplectic generators $x_1, y_1, \dots, x_\ell, y_\ell$ of $D_8^{*\ell}$ all of order 2 and such that $[x_i, y_i] = z$. Let E_0 be the normal subgroup of P generated by z and y_1. As before, let $M = C_P(E_0)$ and $\mathcal{F} = \{F \in \mathcal{A}_p(P)_{>Z(P)} \,|\, F\cap M = Z(P)\}$. A subgroup $F \in \mathcal{F}$ is generated by z and an element $x_1y_1^kxc^t$ with $k, t \in \{0,1\}$ and x is in the subgroup D generated by the elements x_j, y_j with $2 \le j \le \ell$. Since F is elementary abelian, we have

$$1 = (x_1y_1^kxc^t)^2 = z^kx^2z^t$$

Therefore, $k = t$ if $x^2 = 1$, and $k \ne t$ if $x^2 = z$. An element $x \in D$ with $x^2 = 1$ defines thus two subgroups $\langle z, x_1y_1xc\rangle$ and $\langle z, x_1x\rangle$ in $\mathcal{F}$. If $x^2 = z$, then x defines two subgroups $\langle z, x_1y_1x\rangle$ and $\langle z, x_1xc\rangle$ in $\mathcal{F}$. It follows that $\mathcal{F}$ has cardinality $2\cdot 2^{2(\ell-1)} = 2^{2\ell-1}$.

Let $F = \langle z, x_1y_1^kxc^t\rangle \in \mathcal{F}$. If $k = t$, we may assume without loss of generality that $x = x_2$ or $x = 1$. Then $C_M(F)$ is generated by x_2, y_2y_1, respectively

x_2, y_2 if $x = 1$, c and the generators x_j, y_j for $j = 3, \ldots, \ell$. If $k \neq t$, then we may assume that $x = x_2y_2$ and $C_M(F)$ is then generated by x_2y_2, y_2y_1, c and the generators x_j, y_j for $j = 3, \ldots, \ell$. In both cases, $C_M(F)$ is isomorphic to $D_8^{*(\ell-1)} * C_4$.

It follows that $\mathcal{A}_p(D_8^{*\ell} * C_4)_{\geq 2}$ has the homotopy type of a wedge of $2^{2\ell-1}$ copies of the suspension of $\mathcal{A}_p(D_8^{*(\ell-1)} * C_4)_{\geq 2}$. The result follows by an induction argument.

c) If $P = Q_8$, then $\mathcal{A}_p(P)_{\geq 2}$ is empty, hence is a sphere of dimension -1. Suppose now $\ell \geq 1$ and $P = D_8^{*\ell} * Q_8$. Let z be a generator of $Z(P)$ and let $x_1, y_1, \ldots, x_\ell, y_\ell$ be symplectic generators of $D_8^{*\ell}$ all of order 2 such that $[x_i, y_i] = z$. As before, we let $E_0 = \langle z, y_1 \rangle$ and $M = C_P(E_0)$. A subgroup $F \in \mathcal{F} = \{F \in \mathcal{A}_p(P)_{>Z(P)} \mid F \cap M = Z(P)\}$ is generated by z and element $x_1y_1^kxs$ with $k \in \{0, 1\}$, x is in the subgroup D generated by $x_2, y_2, \ldots, x_\ell, y_\ell$ and s is in the subgroup Q_8. Since F is elementary abelian we have

$$1 = (x_1y_1^kxs)^2 = z^kx^2s^2.$$

We have thus

$$k = \begin{cases} 0 & \text{if either } x^2 = 1 = s^2, \text{ or } x^2 = z = s^2. \\ 1 & \text{if either } x^2 = 1 \text{ and } s^2 = z, \text{ or } x^2 = z \text{ and } s^2 = 1. \end{cases}$$

The subgroup F is thus determined by the choice of an element $x \in D$ and an element $s \in Q_8$, both modulo $Z(P)$. It follows that $\mathcal{F}$ has cardinality $2^{2\ell}$.

If $F = \langle z, x_1x \rangle$ with $x^2 = 1$, then we may assume without loss of generality that $x = x_2$ or $x = 1$. In this case $C_M(F)$ is generated by x_2, y_1y_2, respectively x_2, y_2 if $x = 1$, Q_8 and the generators x_j, y_j for $j = 3, \ldots, \ell$.

If $F = \langle z, x_1y_1x \rangle$ with $x^2 = z$, then we may assume that $x = x_2y_2$. In this case $C_M(F)$ is generated by x_2y_2, y_2y_1, Q_8 and the generators x_j, y_j for $j = 3, \ldots, \ell$.

If $F = \langle z, x_1y_1xs \rangle$ with $s^2 = z$, then we may assume that $x = x_2$ or $x = 1$. There exists an element $s' \in Q_8$ such that $[s, s'] = z$ and $C_M(F)$ is generated by x_2, y_2y_1, respectively x_2, y_2 if $x = 1$, s,$s'y_1$ and the generators x_j, y_j for $j = 3, \ldots, \ell$.

If $F = \langle z, x_1xs \rangle$ with $s^2 = z$, then we may assume that $x = x_2y_2$ and $C_M(F)$ is generated by x_2y_2, y_1y_2, s,$s'y_1$, where $s' \in Q_8$ is such that $[s, s'] = z$, and the generators x_j, y_j for $j = 3, \ldots, \ell$.

In all cases, the centralizer $C_M(F)$ is isomorphic to $D_8^{*(\ell-1)} * Q_8$. It follows that $\mathcal{A}_p(D_8^{*\ell} * Q_8)_{\geq 2}$ has the homotopy type of a wedge of $2^{2\ell}$ copies of the suspension of $\mathcal{A}_p(D_8^{*(\ell-1)} * Q_8)_{\geq 2}$. The result follows by an induction argument.

□

Recall that P is assumed to be a 2-group with a cyclic Frattini subgroup and a cyclic center. If $|\Phi(P)| > 2$, it follows from the classification theorems 1.3.26 and 1.3.37, that P is isomorphic to $D_8^{*\ell} * S$, where $\ell \geq 0$ and S is one of the following groups: $C_{2^{m+1}}$, $M_{2^{m+2}}$, $D_{2^{m+2}}$, $SD_{2^{m+2}}$, $Q_{2^{m+2}}$, $D^+_{2^{m+3}}$, $Q^+_{2^{m+3}}$, $D^+_{2^{m+3}} * C_4$, $D_{2^{m+2}} * C_4$, $SD_{2^{m+2}} * C_4$ all with $m > 1$.

The computation of the homotopy type of $\mathcal{A}_p(P)_{\geq 2}$ can be made by a case by case study. When the Frattini subgroup is central, the result is almost immediate.

Lemma 2.3.18. *If $P = D_8^{*\ell} * C_{2^{m+1}}$ with $\ell \geq 0$ and $m > 1$, then $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of 2^{ℓ^2} spheres of dimension $\ell - 1$.*

Proof. If $\ell = 0$, i.e P is cyclic, the result is clear. Otherwise, we have that $\Omega_1(P) = D_8^{*\ell} * C_4$ and the result follows from the preceding lemma. □

Lemma 2.3.19. *If $P = D_8^{*\ell} * M_{2^{m+2}}$ with $\ell \geq 0$ and $m > 1$, then $\mathcal{A}_p(P)_{\geq 2}$ is contractible.*

Proof. If $\ell = 0$, i.e. $P = M_{2^{m+2}}$, there is only one elementary abelian subgroup of rank 2 in P, so that $\mathcal{A}_p(P)_{\geq 2}$ is contractible in this case. If $\ell \geq 1$, the result follows directly from the fact that the center of $\Omega_1(P) = (D_8^{*\ell} * C_4) \times C_2$ is not cyclic. □

It remains then to treat the following cases:

$$D_{2^{m+2}}, SD_{2^{m+2}}, Q_{2^{m+2}}, D^+_{2^{m+3}}, Q^+_{2^{m+3}}, D_{2^{m+2}} * C_4, SD_{2^{m+2}} * C_4, D^+_{2^{m+3}} * C_4 \tag{2.6}$$

Let P be a 2-group of the form $D_8^{*\ell} * S$ with $\ell \geq 0$ and S is one of the group in the list (2.6). The method to determine the homotopy type of $\mathcal{A}_p(P)_{\geq 2}$ goes as follows. Let z be a generator of the unique subgroup of order 2 of $Z(P)$ and let $x_1, y_1, \ldots, x_\ell, y_\ell$ be symplectic generators of the subgroup $D_8^{*\ell}$ all of order 2 and such that $[x_i, y_i] = z$ for all $i = 1, \ldots, \ell$. We would like to apply the Bouc-Thévenaz Wedge Decomposition Formula:

$$\mathcal{A}_p(P)_{\geq 2} \simeq \bigvee_{F \in \mathcal{F}} \Sigma \mathcal{A}_p(C_M(F))_{\geq 2}.$$

We choose E_0 to be the normal subgroup of P generated by z and y_1. The centralizer M of E_0 in P is generated by $z, y_1, x_2, y_2, \ldots, x_\ell, y_\ell$ and S. A subgroup F in $\mathcal{F} = \{F \in \mathcal{A}_p(P)_{>Z(P)} \,|\, F \cap M = Z(P)\}$ is generated by z and an element $g = x_1 y_1^k x s$ with $k \in \{0, 1\}$, x is in the subgroup D generated by x_j, y_j for $2 \leq j \leq \ell$ and s is in S. Since F is elementary abelian, we have $1 = g^2 = z^k x^2 s^2$. As a consequence, s must have order at most 4. Now, if we are given an element x in D and an element s in S of order at most 4, then we can define a subgroup $F(x, s)$ in $\mathcal{F}$ by $F(x, s) = \langle z, x_1 y_1^k x s \rangle$ where k is chosen such that $k = 1$ if $x^2 s^2 = z$ and $k = 0$ if $x^2 s^2 = 1$. If $x' \in D$ and $s' \in S$ with s' of order at most 4, then $F(x, s) = F(x', s')$ if and only if $xs = x's'$ or $xs = x's'z$. It follows that $x = x'$ or $x = x'z$ and $s = s'$ or $s = s'z$. There are thus 4 different pairs (x, s) that define the same subgroup in $\mathcal{F}$. This allows us to determine the number of subgroups in $\mathcal{F}$.

If c denotes the number of element of S of order at most 4, then

$$|\mathcal{F}| = \frac{1}{4} c \cdot 2^{2(l-1)+1} \tag{2.7}$$

If $F = \langle z, x_1 y_1^k xs\rangle$ is in $\mathcal{F}$ then $C_M(F)$ is the centralizer in M of the element $x_1 y_1^k xs$. To apply the Bouc-Thévenaz Wedge Decomposition Formula, we need to determine now exactly these centralizers. This is what we are going to do in what follows. In the following proofs, we will keep the notation as above.

Lemma 2.3.20. *Let $P = D_{2^{m+2}}$ with $m \geq 1$. Then $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of $2^m - 1$ spheres of dimension 0.*

Proof. The elementary abelian subgroups of $D_{2^{m+2}}$ have order at most 4. Furthermore, $D_{2^{m+2}}$ has a unique cyclic subgroup of order 4 containing the center and all other subgroups of order 4 containing the center are elementary abelian. It follows that $\mathcal{A}_p(P)_{\geq 2}$ consists of 2^m isolated points, hence has the homotopy type of a wedge of $2^m - 1$ spheres of dimension 0. $\square$

Lemma 2.3.21. *If $P = D_8^{*\ell} * D_{2^{m+2}}$ with $m > 1$ and $\ell \geq 1$, then $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of $2^{\ell^2}(2^{m-1}(2^\ell + 1) - 1)$ spheres of dimension ℓ.*

Proof. We keep the notation as above and in particular here $S = D_{2^{m+2}}$. Let a, u be generators of S with a of order 2, u of order 2^{m+1} and $aua^{-1} = u^{-1}$. The elements of order 2 in S are those of the form au^i with $i = 0, \ldots, 2^{m+1} - 1$ and there are two elements of order 4, namely $w = u^{2^{m-1}}$ and $w^{-1} = wz$.

Suppose first that $\ell = 1$ and let $F \in \mathcal{F}$. In this case, F is generated by z and an element $g = x_1 y_1^k s$ with $s \in S$.

If $s = 1$ or $s = z$, then $C_M(F) = S$. If $s = w$ or $s = w^{-1}$, then $C_M(F)$ is generated by u and $y_1 a$, hence is isomorphic to $D_{2^{m+2}}$. If $s \neq z$ and s has order 2, we may assume without loss of generality that $s = a$. But then $C_M(F)$ is generated by a and $y_1 w$, hence is isomorphic to D_8. There are thus two subgroups in $\mathcal{F}$ with a centralizer in M isomorphic to $D_{2^{m+2}}$, namely the subgroups $\langle z, x_1\rangle$ and $\langle z, x_1 y_1 w\rangle$. And there are 2^m subgroups in $\mathcal{F}$ with centralizer in M isomorphic to D_8, namely the subgroups of the form $\langle z, au^i\rangle$ with $i \geq 0$. It follows then from the Bouc-Thévenaz Wedge Decomposition Formula that $\mathcal{A}_p(D_8 * D_{2^{m+2}})_{\geq 2}$ has the homotopy type of the wedge of 2 copies of the suspension of $\mathcal{A}_p(D_{2^{m+2}})_{\geq 2}$ and 2^m copies of the suspension of $\mathcal{A}_p(D_8)_{\geq 2}$. By Lemma 2.3.17 and Lemma 2.3.20, we obtain that $\mathcal{A}_p(D_8 * D_{2^{m+2}})_{\geq 2}$ has the homotopy type of $2(2^m - 1) + 2^m = 2(2^{m-1}(2 + 1) - 1)$ spheres of dimension 1.

Suppose now $\ell > 1$ and let $F = \langle z, g\rangle \in \mathcal{F}$ with $g = x_1 y_1^k xs$. If $x \neq z$ and x has order 2 we may suppose without loss of generality that $x = x_2$ and if x has order 4 we may suppose that $x = x_2 y_2$. If $x \neq z$ and $x \neq 1$, we may thus suppose that $x = x_2 y_2^\varepsilon$ for some $\varepsilon \in \{0, 1\}$.

Suppose first that $x \neq 1$ and s has order 4. We may assume that $s = w$ and we claim that the centralizer in M of $g = x_1 y_1^k x_2 y_2^\varepsilon w$ is generated by the following elements:

$$x_j, y_j, \text{ for } 3 \leq j \leq l, \tag{2.8}$$
$$x_2 y_2^\varepsilon, y_1 y_2, \tag{2.9}$$
$$y_1 a, u. \tag{2.10}$$

These elements all lie in M which is the subgroup generated by all generators of P except x_1 and easy but technical calculations show that they centralize g.

If $h = y_1^{\beta_1} x_2^{\alpha_2} y_2^{\beta_2} \cdots x_\ell^{\alpha_l} y_\ell^{\beta_\ell} a^\gamma u^\delta$ is an element of M with $\beta_1, \alpha_j, \beta_j, \gamma, \delta \in \{0,1\}$, then

$$\begin{aligned} hgh^{-1} &= (y_1^{\beta_1} x_1 y_1^{-\beta_1}) y_1^k (y_2^{\beta_2} x_2 y_2^{-\beta_2})(x_2^{\alpha_2} y_2^{\varepsilon} x_2^{-\alpha_2})(a^\gamma w a^{-\gamma}) \\ &= (z^{\beta_1} x_1) y_1^k (z^{\beta_2} x_2)(z^{\alpha_2 \varepsilon} y_2^{\varepsilon})(z^\gamma w) \\ &= g z^{\beta_1 + \beta_2 + \alpha_2 \varepsilon + \gamma} \end{aligned}$$

If h centralizes g, then $\beta_1 = \beta_2 + \alpha_2\varepsilon + \gamma + 2\mu$ for some $\mu \geq 0$ and h can be rewritten

$$h = (x_2 y_2^{\varepsilon})^{\alpha_2} (y_1 y_2)^{\beta_2 + \alpha_2 \varepsilon} (y_1 a)^\gamma x_3^{\alpha_3} \cdots y_\ell^{\beta_\ell} u^\delta$$

and our claim is proved.

The subgroup generated by $x_2 y_2^{\varepsilon}$ and $y_1 y_2$ is isomorphic to D_8, since their commutator is z and $y_1 y_2$ has order 2. The subgroup generated by u and $y_1 a$ is easily seen to be isomorphic to $D_{2^{m+2}}$. It follows that $C_M(F)$ is isomorphic to $D_8^{*(\ell-1)} * D_{2^{m+2}}$. It is not difficult to adapt the above argument when x or s is central and in these cases also $C_M(F)$ is isomorphic to $D_8^{*(\ell-1)} * D_{2^{m+2}}$.

Suppose now that $s \neq z$ and s has order 2. Without loss of generality, we may suppose that $s = a$. In this situation, the centralizer in M of $g = x_1 y_1^k x_2 y_2^{\varepsilon} a$ is generated by the following elements

$$x_j, y_j, \text{ for } 3 \leq j \leq l, \tag{2.11}$$

$$x_2 y_2^{\varepsilon}, y_1 y_2, \tag{2.12}$$

$$a, y_1 w. \tag{2.13}$$

It is not difficult to see that these elements centralize g and an argument as before shows that these elements actually generate $C_M(g)$. The subgroup generated by a and $y_1 w$ is isomorphic to D_8, so that this time $C_M(F)$ is isomorphic to $D_8^{*\ell}$. As before, this remains true if $x = 1$ or $x = z$.

Let us summarize the situation. We have seen that the choice of a pair (x, s) with $s = 1$, $s = z$ or s of order 4 gives a subgroup F in $\mathcal{F}$ with $C_M(F)$ isomorphic to $D_8^{*(\ell-1)} * D_{2^{m+2}}$. There are $2^{2(l-1)+1} \cdot 4$ such pairs, hence $2^{2\ell-1}$ subgroups in $\mathcal{F}$ have a centralizer isomorphic to $D_8^{*(\ell-1)} * D_{2^{m+2}}$.

The choice of a pair (x, s) with $s \neq z$ and s of order 2 gives a subgroup F in $\mathcal{F}$ with $C_M(F)$ isomorphic to $D_8^{*\ell}$. There are $2^{2(\ell-1)+1} \cdot 2^{m+1}$ such pairs, hence $2^{2(\ell-1)+m}$ subgroups in $\mathcal{F}$ have a centralizer in M isomorphic to $D_8^{*\ell}$.

The dimension and the number of spheres in $\mathcal{A}_p(P)_{\geq 2}$ can now be computed by a recursive use of the Bouc-Thévenaz wedge decomposition, together with the results of Lemma 2.3.17. □

The proofs in the other cases are relatively similar, so that we will give less details from now on.

Lemma 2.3.22. *Let $P = SD_{2^{m+2}}$ with $m > 1$, then $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of $2^{m-1} - 1$ spheres of dimension 0.*

Proof. Let a, u be generators of P such that u has order 2^{m+1}, a has order 2 and $aua^{-1} = u^{-1+2^m}$. The center of P is generated by $z = u^{2^m}$. The elements of the form au^i have order 2 if i is even and 4 if i is odd. It follows that P has 2^m elements of order 2 distinct from z. It follows that $\mathcal{A}_p(P)_{\geq 2}$ consists of 2^{m-1} isolated points and the lemma is proved. □

Lemma 2.3.23. *Let $P = D_8^{*\ell} * SD_{2^{m+2}}$ with $\ell \geq 1$ and $m > 1$, then $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of $2^{\ell^2}(2^{m-2}(2^\ell+1)-1)$ spheres of dimension ℓ and $2^{\ell^2}(2^{m-2}(2^\ell-1))$ spheres of dimension $\ell-1$.*

Proof. With our above notation, $S = SD_{2^{m+2}}$. Let a, u be generators of $SD_{2^{m+2}}$ with u of order 2^{m+1}, a of order 2 and $aua^{-1} = u^{-1+2^m}$. Let $F = \langle z, g\rangle \in \mathcal{F}$ with $g = x_1y_1^kxs$. The elements of S of the form au^i with i even have order 2. The elements of the form au^i with i odd and the elements $w = u^{2^{m-1}}$ and w^{-1} are the elements of order 4 of S.

If $x \neq 1$ and $x \neq z$, we may assume that $x = x_2y_2^\varepsilon$. Suppose first that s has order 4. Without loss of generality we may assume $s = au$ or $s = w$. If $s = w$, then $C_M(F)$ is generated by the following elements:

$$x_j, y_j, \text{ for } 3 \leq j \leq l, \tag{2.14}$$
$$x_2y_2^\varepsilon, y_1y_2, \tag{2.15}$$
$$y_1a, u. \tag{2.16}$$

Note that the subgroup generated by u and y_1a is isomorphic to $SD_{2^{m+2}}$. If $s = au$, then $C_M(F)$ is generated by the following elements:

$$x_j, y_j, \text{ for } 3 \leq j \leq l, \tag{2.17}$$
$$x_2y_2^\varepsilon, y_1y_2, \tag{2.18}$$
$$au, wy_1. \tag{2.19}$$

The subgroup generated by au and wy_1 is isomorphic to Q_8, since both generators have order 4 and their commutator equals z.

Suppose now that $s \neq z$, $s \neq 1$ and s has order 2. Without loss of generality, we may suppose that $s = a$. The centralizer of M in F is then generated by the following elements:

$$x_j, y_j, \text{ for } 3 \leq j \leq l, \tag{2.20}$$
$$x_2y_2^\varepsilon, y_1y_2, \tag{2.21}$$
$$a, y_1w. \tag{2.22}$$

The subgroup generated by a and y_1w is isomorphic to D_8.

There are $2^{2\ell-1}(2^{m-1}+1)$ subgroups in $\mathcal{F}$ and among them $2^{2\ell-1}$ have a centralizer in M isomorphic to $D_8^{*\ell-1} * SD_{2^{m+2}}$, $2^{2\ell+m-3}$ have a centralizer in M isomorphic to $D_8^{*\ell-1} * D_8$ and $2^{2\ell+m-3}$ have a centralizer in M isomorphic to $D_8^{*\ell-1} * Q_8$. The lemma follows from a recursive use of the Bouc-Thévenaz Wedge Decomposition Formula, as well as Lemma 2.3.17. □

Lemma 2.3.24. *Let $P = Q_{2^{m+2}}$ with $m \geq 1$, then $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a sphere of dimension -1.*

Proof. Recall that the subgroup $Q_{2^{m+2}}$ has no non-cyclic abelian subgroups (see [14, Theorem 5.4.10]), hence $\mathcal{A}_p(P)_{\geq 2}$ is empty. □

Lemma 2.3.25. *Let $P = D_8^{*\ell} * Q_{2^{m+2}}$ with $\ell \geq 1$ and $m > 1$. Then $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of $2^{\ell^2}(2^{m-1}(2^\ell - 1) + 1)$ spheres of dimension $\ell - 1$.*

Proof. Let $F = \langle z, g\rangle \in \mathcal{F}$ with $g = x_1 y_1^k x s$ with $s \in S = Q_{2^{m+2}}$. Let b, u be generators of S with u of order 2^{m+1} and b of order 4 with $bub^{-1} = u^{-1}$. Let also $w = u^{2^{m-1}}$. If $s = z$ or $s = 1$, then $C_M(F)$ is isomorphic to $D_8^{*(\ell-1)} * Q_{2^{m+2}}$. If $s = w$ or $s = w^{-1} = wz$, then $C_M(F)$ is generated by the following elements

$$x_j, y_j, \text{ for } 3 \leq j \leq l, \tag{2.23}$$
$$x_2 y_2^{\varepsilon}, y_1 y_2, \tag{2.24}$$
$$y_1 b, u. \tag{2.25}$$

The subgroup generated by u and $y_1 b$ is isomorphic to $Q_{2^{m+2}}$. Suppose now that s has order 4, but $s \neq w$ and $s \neq w^{-1}$. We may assume that $s = b$ and then $C_M(F)$ is generated by the following elements:

$$x_j, y_j, \text{ for } 3 \leq j \leq l, \tag{2.26}$$
$$x_2 y_2^{\varepsilon}, y_1 y_2, \tag{2.27}$$
$$b, y_1 w \tag{2.28}$$

The subgroup generated by b and $y_1 w$ is isomorphic to Q_8, hence $C_M(F)$ is isomorphic to $D_8^{*(\ell-1)} * Q_8$.

We have now $2^{2\ell-1}$ subgroups in $\mathcal{F}$ with a centralizer in M isomorphic to $D_8^{*\ell-1} * Q_{2^{m+2}}$ and $2^{2\ell+m-2}$ subgroups in $\mathcal{F}$ with a centralizer in M isomorphic to $D_8^{*\ell-1} * Q_8$. As usual, the lemma follows now from a recursive use of the Bouc-Thévenaz Wedge Decomposition Formula, as well as Lemma 2.3.17. □

For the remaining cases, we will choose a more appropriate normal subgroup E_0 to simplify the calculations. The method remains the same.

Lemma 2.3.26. *Let $P = D^+_{2^{m+3}}$ with $m > 1$, then $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of 2^{m-1} spheres of dimension 0.*

Proof. Let a, b, u be generators of P with a, b of order 2, u of order 2^{m+1}, $[a, b] = 1$, $aua^{-1} = u^{1+2^m}$ and $bub^{-1} = u^{-1}$. Let $w = u^{2^{m-1}}$ and $z = w^2 = u^{2^m}$. Let E_0 be the normal subgroup of P generated by a and z. The centralizer M of E_0 in P is generated by a, b and u^2. If F is a subgroup in $\mathcal{F} = \{F \in \mathcal{A}_p(P)_{>Z(P)} \,|\, F \cap M = Z(P)\}$, then F is generated by z and an element g of the form $g = b^i a^j u^k$ for some $i, j \in \{0, 1\}$ and $0 \leq k \leq 2^{m+1} - 1$ with k odd. Since F is elementary abelian, we have $g^2 = 1$, hence g has the form $u^k b$ with k odd. The centralizer in M of such an element is the cyclic subgroup of order 4 generated by aw. There are thus 2^{m-1} subgroups F in $\mathcal{F}$ all with a centralizer in M cyclic of order 4. The results follows then from the Bouc-Thévenaz Wedge Decomposition Formula. □

Lemma 2.3.27. *Let $P = D_8^{*\ell} * D^+_{2^{m+3}}$ with $\ell \geq 1$ and $m > 1$. Then $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of $2^{(\ell+1)^2+m-2}$ spheres of dimension ℓ.*

Proof. Let a, b, u be generators of $D^+_{2^{m+3}}$ with a, b of order 2, u of order 2^{m+1}, $[a, b] = 1$, $aua^{-1} = u^{1+2^m}$ and $bub^{-1} = u^{-1}$. Let $w = u^{2^{m-1}}$ and $z = w^2 = u^{2^m}$. Let E_0 be the normal subgroup of P generated by a and z and let M be the centralizer of E_0 in P. We have

$$M = \langle x_1, y_1, \dots, x_\ell, y_\ell, a, b, u^2\rangle.$$

A subgroup $F \in \mathcal{F} = \{F \in \mathcal{A}_p(P)_{>Z(P)} \mid F \cap M = Z(P)\}$ is generated by z and an element $g = xa^ib^ju^k$ of order 2 and with k odd. Remark that the element au^k with k odd have order 2^{m+1}, so that we can restrict to the following cases.

If $g = bu$, then then $C_M(F)$ is generated by all the x_i, y_i and the elements aw. It follows that $C_M(F)$ is isomorphic to $D_8^{*\ell} * C_4$.

If $g = x_1bu$, then $C_M(F)$ is generated by x_j, y_j with $j \neq 1$ and the elements x_1,y_1w and aw. It follows that $C_M(F)$ is isomorphic to $D_8^{*\ell} * C_4$.

If $g = x_1y_1abu$, then $C_M(F)$ is generated by x_j, y_j with $j \neq 1$ and the elements x_1a,y_1a and aw. It follows that $C_M(F)$ is isomorphic to $D_8^{*\ell} * C_4$.

There are thus $2^{2\ell+m-1}$ subgroups in $\mathcal{F}$ all with centralizer in M isomorphic to $D_8^{*\ell} * C_4$. The result follows now from the Bouc-Thévenaz Wedge Decomposition Formula together with Lemma 2.3.17. □

Lemma 2.3.28. *Let $P = Q^+_{2^{m+3}}$ with $m > 1$. Then $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of 2^{m-1} spheres of dimension 0.*

Proof. Let a, b, u be generators of P with a of order 2, b of order 4 and u of order 2^{m+1} and with $[a, b] = 1$, $aua^{-1} = u^{1+2^m}$ and $bub^{-1} = u^{-1}$. The elementary abelian subgroups of rank 2 in P containing $Z(P)$ are generated by $z = u^{2^m}$ and either a or an element abu^i with i odd. No two of these elements commute, so that $\mathcal{A}_p(P)_{>Z(P)}$ is a wedge of 2^{m-1} spheres of dimension 0. □

Lemma 2.3.29. *Let $P = D_8^{*\ell} * Q^+_{2^{m+3}}$ with $\ell \geq 1$ and $m > 1$. Then $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of $2^{(\ell+1)^2+m-2}$ spheres of dimension ℓ.*

Proof. Let a, b, u be generators of $Q^+_{2^{m+3}}$, where a has order 2, u has order 2^{m+1}, b has order 4 with $b^2 = u^{2^m}$, and where $[a, b] = 1$, $aua^{-1} = u^{1+2^m}$ and $bub^{-1} = u^{-1}$. Let $w = u^{2^{m-1}}$ and $z = b^2 = w^2 = u^{2^m}$. Let E_0 be the normal subgroup of P generated by a and z and let M be the centralizer of E_0 in P. We have

$$M = \langle x_1, y_1, \dots, x_\ell, y_\ell, a, b, u^2\rangle.$$

A subgroup $F \in \mathcal{F} = \{F \in \mathcal{A}_p(P)_{>Z(P)} \mid F \cap M = Z(P)\}$ is generated by z and an element $g = xa^ib^ju^k$ of order 2 and with k odd. We can thus restrict to the following cases.

If $g = x_1y_1bu$, then $C_M(F)$ is generated by x_j, y_j with $j \neq 1$ and the elements x_1a,y_1a and aw. It follows that $C_M(F)$ is isomorphic to $D_8^{*\ell} * C_4$.

If $g = abu$, then $C_M(F)$ is generated by x_j, y_j with $j = 1, \dots, \ell$, and the element aw. It follows that $C_M(F)$ is isomorphic to $D_8^{*\ell} * C_4$.

If $g = x_1abu$, then $C_M(F)$ is generated by x_j, y_j with $j \neq 1$ and the elements x_1a,y_1a and aw. It follows that $C_M(F)$ is isomorphic to $D_8^{*\ell} * C_4$.

There are thus $2^{2\ell+m-1}$ subgroups in $\mathcal{F}$ all with centralizer isomorphic to $D_8^{*\ell} * C_4$. The result follows now from the Bouc-Thévenaz Wedge Decomposition Formula together with Lemma 2.3.17. $\square$

Lemma 2.3.30. *Let $P = D_8^{*\ell} * D_{2^{m+2}} * C_4$ with $\ell \geq 0$ and $m > 1$, then $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of $2^{(\ell+1)^2+m-1}$ spheres of dimension ℓ.*

Proof. Let u, v be generators of $D_{2^{m+2}}$ with u of order 2^{m+1}, a of order 2 and $aua^{-1} = u^{-1}$. Let $w = u^{2^{m-1}}$ and $z = w^2 = u^{2^m}$. Let c be a generator of the subgroup C_4 and let E_0 be the subgroup generated by z and wc. The centralizer M of E_0 in P has the following generators:

$$M = \langle x_1, y_1, \ldots, x_\ell, y_\ell, u, c\rangle.$$

A subgroup F in $\mathcal{F}$ is generated by z and an element $g = xau^k c^l$ with x in the subgroup $D_8^{*\ell}$. Each of these subgroups is obtained by choosing k and x and by letting $l = 1$ if x has order 4. There are thus $2^{2\ell+m}$ such subgroups. To determine the centralizer, we may assume without loss of generality that $x = 1$ or $x = x_\ell y_\ell^\varepsilon$ with $\varepsilon \in \{0, 1\}$. The centralizer of g in M is generated by c and the following elements:

$$x_j, y_j \text{ for } j = 1, \ldots, \ell - 1,$$
$$x_\ell y_\ell^\varepsilon, y_\ell w \text{ if } x \neq 1 \text{ respectively } x_\ell, y_\ell \text{ if } x = 1,$$

The subgroup generated by $x_\ell y_\ell^\varepsilon$ and $y_\ell w$ may be replaced by the subgroup generated by $x_\ell y_\ell^\varepsilon$ and $y_\ell wc$ so that it is isomorphic to D_8. This shows that the centralizer of F in M is isomorphic to $D_8^{*\ell} * C_4$. The lemma follows now from the Bouc-Thévenaz Wedge Decomposition Formula and Lemma 2.3.17. $\square$

The proof in the case $P = D_8^{*\ell} * SD_{2^{m+2}} * C_4$ is very similar to the previous one, so that we will not include it.

Lemma 2.3.31. *Let $P = D_8^{*\ell} * SD_{2^{m+2}} * C_4$ with $\ell \geq 0$ and $m > 1$, then $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of $2^{(\ell+1)^2+m-1}$ spheres of dimension ℓ.*

Lemma 2.3.32. *Let $P = D_8^{*\ell} * D^+_{2^{m+3}} * C_4$ with $\ell \geq 0$ and $m > 1$, then $\mathcal{A}_p(P)_{\geq 2}$ is contractible.*

Proof. Let a, b, u be generators of the subgroup $D^+_{2^{m+3}}$ with a, b of order 2, u of order 2^{m+1}, $[a, b] = 1$, $aua^{-1} = u^{1+2^m}$ and $bub^{-1} = u^{-1}$. Let $w = u^{2^{m-1}}$ and $z = w^2 = u^{2^m}$. Let c be the generator of the subgroup C_4 and let E_0 be the normal subgroup of P generated by z and wc. The centralizer M of E_0 in P has the following generators

$$M = \langle x_1, y_1, \ldots, x_\ell, y_\ell, u, a, c\rangle.$$

A subgroup F in $\mathcal{F}$ is generated by z and an element $g = xa^k bu^i c^t$. If i is even, then a centralizes g and if i is odd, then wac centralizes g. But these two elements are central in M, hence $C_M(F)$ has a central elementary abelian subgroup of rank 2. It follows that $\mathcal{A}_p(C_M(F))_{\geq 2}$ is contractible for all $F \in \mathcal{F}$. The lemma follows from the Bouc-Thévenaz Wedge Decomposition Formula. $\square$

Let $\ell \geq 1$ and $m > 1$. In the table 2.1 located on page 74, the reader will find the number and dimension of spheres occurring in the poset $\mathcal{A}_p(P)_{\geq 2}$ for any non-abelian p-group P with $Z(P)$ and $\Phi(P)$ cyclic of order p^m. For some (small) values of ℓ and m, these numerical results have been verified using the programming language GAP [13].

As a corollary to all these computations, we obtain that p-groups with cyclic derived subgroup give a positive answer to the Question 2.1.2 raised by Bouc and Thévenaz.

Corollary 2.3.33. *Let P be a p-group with cyclic derived subgroup. Then*

a) If p is odd $\mathcal{A}_p(P)_{\geq 2}$ is homotopy equivalent to a wedge of spheres of the same dimension.

b) If $p = 2$, then $\mathcal{A}_p(P)_{\geq 2}$ is homotopy equivalent to a wedge of spheres of the same dimension, or of two consecutive dimensions.

P	$\mathcal{A}_p(P)_{\geq 2}$
$X_{p^{2\ell+1}}$	p^{ℓ^2} spheres of dimension $\ell - 1$
$X_{p^{2(\ell-1)+1}} * X_{p^3}^-$	contractible
$X_{p^{2\ell+1}} * C_{p^m}$	p^{ℓ^2} spheres of dimension $\ell - 1$
$X_{p^{2(\ell-1)+1}} * M_{p^{m+2}}$	contractible
$D_8^{*\ell}$	$2^{\ell(\ell-1)}$ spheres of dimension $\ell - 1$
$D_8^{*\ell} * C_4$	2^{ℓ^2} spheres of dimension $\ell - 1$
$D_8^{*(\ell-1)} * Q_8$	$2^{\ell(\ell-1)}$ spheres of dimension $\ell - 2$
$D_8^{*\ell} * C_{2^{m+1}}$	2^{ℓ^2} spheres of dimension $\ell - 1$
$D_8^{*(\ell-1)} * M_{2^{m+2}}$	contractible
$D_8^{*(\ell-1)} * D_{2^{m+2}}$	$2^{(\ell-1)^2}(2^{m-1}(2^{(\ell-1)} + 1) - 1)$ spheres of dimension $\ell - 1$
$D_8^{*(\ell-1)} * SD_{2^{m+2}}$	$2^{(\ell-1)^2}(2^{m-2}(2^{(\ell-1)}+1)-1)$ spheres of dimension $\ell-1$ and $2^{(\ell-1)^2}(2^{m-2}(2^{(\ell-1)} - 1))$ spheres of dimension $\ell - 2$
$D_8^{*(\ell-1)} * Q_{2^{m+2}}$	$2^{(\ell-1)^2}(2^{m-1}(2^{(\ell-1)} - 1) + 1)$ spheres of dimension $\ell - 2$
$D_8^{*(\ell-1)} * D_{2^{m+2}} * C_4$	2^{ℓ^2+m-1} spheres of dimension $\ell - 1$
$D_8^{*(\ell-1)} * SD_{2^{m+2}} * C_4$	2^{ℓ^2+m-1} spheres of dimension $\ell - 1$
$D_8^{*(\ell-1)} * D_{2^{m+3}}^+$	2^{ℓ^2+m-2} spheres of dimension $\ell - 1$
$D_8^{*(\ell-1)} * Q_{2^{m+3}}^+$	2^{ℓ^2+m-2} spheres of dimension $\ell - 1$
$D_8^{*(\ell-1)} * D_{2^{m+3}}^+ * C_4$	contractible

Table 2.1: Homotopy type of $\mathcal{A}_p(P)_{\geq 2}$ for p-groups P with $Z(P)$ and $\Phi(P)$ cyclic. In this table, $\ell \geq 1$ and $m > 1$.

2.4 Maximal Dimension of spheres

We have seen, that for a p-group P, the poset $\mathcal{A}_p(P)_{\geq 2}$ is homotopy equivalent to a wedge of spheres. The dimension of these spheres cannot be greater than the dimension of the simplicial complex $\mathcal{A}_p(P)_{\geq 2}$. In this section, we will give a sharper bound on the dimension of the spheres depending on the order of the group. More precisely, we show that if P has order p^n, then there are no spheres in dimension greater than or equal to $\lfloor \frac{n-1}{2} \rfloor$. If $n = 2\ell + 1$ is odd, this implies that the maximal dimension of the spheres is $\ell - 1$ and we show furthermore that a p-group of order $p^{2\ell+1}$ has spheres in dimension $\ell - 1$ if and only if P is extraspecial of type I. When n is even we obtain a similar, but weaker result. More precisely, if P has order p^ℓ and $\tilde{H}_{\ell-2}(\mathcal{A}_p(P)_{\geq 2}) \neq 0$, then P has a maximal subgroup extraspecial of type I.

Lemma 2.4.1. *Let P be a p-group with $Z = \Omega_1(Z(P))$ of order p and let $E, F \in \mathcal{A}_p(P)_{>Z}$ with E, F of rank 2, E normal in P and F does not centralize E. Then the subgroup EF is extraspecial of type I and order p^3 with $Z(EF) = Z$ and the following assertions are equivalent, where $M = C_P(E)$:*

a) F is normal in P.

b) $|M : C_M(F)| = p$.

c) $P = C_M(F) \underset{Z}{*} EF$.

Proof. Since E is normal in P and hence in EF, we have $EF/E \cong F/(E \cap F)$. Since F does not centralize E, we have $E \neq F$ and since both E and F contain Z and have rank 2, we must have $E \cap F = Z$. It follows that EF has order p^3. Furthermore, the action of F on E by conjugation induces an action on the quotient E/Z. Since E/Z is cyclic of order p, this action is trivial, so that $fef^{-1} \in eZ$ for all $e \in E$, $f \in F$. It follows that $[EF, EF] = Z$ and since EF is generated by elements of order p, we obtain thus that EF is extraspecial of type I.

We prove now the equivalence of the assertions. If F is normal in P, then $C_P(F)$ has index p in P and hence $|M : C_M(F)| = p$. In this situation, M is generated by $C_M(F)$ and E, since E and F do not commute and thus P is generated by $C_M(F)$ and EF. For the same reason $C_M(F) \cap EF = Z$ and those two subgroups commute, hence P is a central product $C_M(F) \underset{Z}{*} EF$. In this case, F is clearly normal in P and the lemma is proved. □

For any positive real number r, we denote $\lfloor r \rfloor$ the greatest integer n such that $n \leq r$.

Lemma 2.4.2. *If P is a p-group of order p^n, $n \geq 1$, then $\tilde{H}_k(\mathcal{A}_p(P)_{\geq 2}) = 0$ if $k \geq \lfloor \frac{n-1}{2} \rfloor$.*

Proof. The proof goes by induction on n. It is clear for $n = 1, 2, 3$, so we suppose $n \geq 4$ and that the result holds for $1 \leq n' < n$. If $|\Omega_1(Z(P))| > p$, then $\mathcal{A}_p(P)_{\geq 2}$ is contractible and the result holds trivially. If either P is cyclic, or $p = 2$ and P is isomorphic to one of the following groups:

$$D_{2^n},\ Q_{2^n} \text{ or } SD_{2^n} \tag{2.29}$$

with $n \geq 4$, then $\tilde{H}_k(\mathcal{A}_p(P)_{\geq 2}) = 0$ for $k \geq 1$, so that the result holds for these groups. If $Z = \Omega_1(Z(P))$ has order p and P is not cyclic nor one of the groups in (2.29), then by Lemma 2.3.12 we have that P contains a normal subgroup E_0 elementary abelian of rank 2 containing Z and $M = C_P(E_0)$ is maximal in P.

Let $\mathcal{F} = \{F \in \mathcal{A}_p(P)_{\geq 2} \,|\, F \cap M = Z\}$, Proposition 2.3.7 implies in particular that

$$\tilde{H}_k(\mathcal{A}_p(P)_{\geq 2}) \cong \bigoplus_{F \in \mathcal{F}} \tilde{H}_{k-1}(\mathcal{A}_p(C_M(F))_{\geq 2}).$$

For $F \in \mathcal{F}$, we have $C_M(F) < M$, hence $|C_M(F)| = p^r$ with $r \leq n-2$. By induction, we have $\tilde{H}_{k-1}(\mathcal{A}_p(C_M(F))_{\geq 2}) = 0$ if $k-1 \geq \lfloor \frac{n-3}{2} \rfloor = \lfloor \frac{n-1}{2} \rfloor - 1$. Therefore $\tilde{H}_k(\mathcal{A}_p(P)_{\geq 2}) = 0$ if $k \geq \lfloor \frac{n-1}{2} \rfloor$. $\square$

Proposition 2.4.3. *Let P be a p-group. If $|P| = p^{2\ell+1}$ with $\ell \geq 1$, then $\tilde{H}_k(\mathcal{A}_p(P)_{\geq 2}) = 0$ if $k \geq \ell$. Furthermore, $\tilde{H}_{\ell-1}(\mathcal{A}_p(P)_{\geq 2}) \neq 0$ if and only if P is extraspecial of type I.*

Proof. The first assertion, namely $\tilde{H}_k(\mathcal{A}_p(P)_{\geq 2}) = 0$ for $k \geq \ell$, follows directly from Lemma 2.4.2.

Let P be an extraspecial p-group of type I and order $p^{2\ell+1}$, with $\ell \geq 1$. We know from Lemma 2.3.15 and Lemma 2.3.17 that the poset $\mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of p^{ℓ^2}, respectively $2^{\ell(\ell-1)}$ if $p = 2$, spheres of dimension $\ell - 1$. Since $\ell \geq 1$, this implies $\tilde{H}_{\ell-1}(\mathcal{A}_p(P)_{\geq 2}) \neq 0$.

The proof of the converse goes by induction on ℓ. It is clear for $\ell = 1$ and we suppose true for $1 \leq r \leq \ell - 1$ and $|P| = p^{2\ell+1}$, with $\ell \geq 2$. The hypothesis $\tilde{H}_{\ell-1}(\mathcal{A}_p(P)_{\geq 2}) \neq 0$ implies in particular that P is not cyclic, dihedral, quaternion or semidihedral and that $\Omega_1(Z(P))$ is cyclic of order p. It follows that P has a normal elementary abelian subgroup of rank 2 and Proposition 2.3.7 gives then

$$\tilde{H}_{\ell-1}(\mathcal{A}_p(P)_{\geq 2}) \cong \bigoplus_{F \in \mathcal{F}} \tilde{H}_{\ell-2}(\mathcal{A}_p(C_M(F))_{\geq 2}).$$

Since $\tilde{H}_{\ell-1}(\mathcal{A}_p(P)_{\geq 2}) \neq 0$, there exists a subgroup $F_0 \in \mathcal{F}$ such that

$$\tilde{H}_{\ell-2}(\mathcal{A}_p(C_M(F_0))_{\geq 2}) \neq 0.$$

By Lemma 2.4.2 we must then have $\ell - 2 < \lfloor \frac{r-1}{2} \rfloor$, where $|C_M(F_0)| = p^r$. Since $C_M(F_0) < M$, we also have $r \leq 2\ell - 1$ and these two conditions together force r to be equal to $2\ell - 1$.

Now $C_M(F)$ has order $p^{2(\ell-1)+1}$ and $\tilde{H}_{\ell-2}(\mathcal{A}_p(C_M(F_0))_{\geq 2}) \neq 0$, so that by the induction hypothesis $C_M(F_0)$ is extraspecial of type I. By Lemma 2.4.1, P is a central product $P = C_M(F_0) * (E_0F_0)$ and E_0F_0 is extraspecial of type I, showing that P is extraspecial of type I. $\square$

Proposition 2.4.4. *Let P be a p-group of order $p^{2\ell}$, with $\ell \geq 2$. Then $\tilde{H}_k(\mathcal{A}_p(P)_{\geq 2}) = 0$ if $k \geq \ell - 1$. Moreover, if $\tilde{H}_{\ell-2}(\mathcal{A}_p(P)_{\geq 2}) \neq 0$, then P has a maximal subgroup which is extraspecial of type I.*

Proof. The first assertion, namely $\tilde{H}_k(\mathcal{A}_p(P)_{\geq 2}) = 0$ for $k \geq \ell - 1$, follows directly from Lemma 2.4.2 since $\lfloor \frac{2\ell-1}{2} \rfloor = \ell - 1$.

Let now P be a group such that $\tilde{H}_{\ell-2}(\mathcal{A}_p(P)_{\geq 2}) \neq 0$. Since $\ell \geq 2$, we have in particular that $Z = \Omega_1(Z(P))$ has order p.

The proof goes by induction on ℓ and we suppose first $\ell = 2$, i.e. $|P| = p^4$. We have thus by assumptions that

$$\tilde{H}_0(\mathcal{A}_p(P)_{\geq 2}) \neq 0. \tag{2.30}$$

This condition (2.30) implies in particular that P is not cyclic and that P is not quaternion if $p = 2$. If $P = D_{16}$ or SD_{16}, then P contains a maximal subgroup isomorphic to D_8 so that the result holds for these groups. Note that (2.30) holds in this case (see Lemma 2.3.20 and Lemma 2.3.22).

We may assume now that P is not cyclic and furthermore that P is not dihedral, semi-dihedral nor quaternion if $p = 2$. It follows now that P has a normal elementary abelian subgroup E_0 of rank 2 with $Z \leq E_0$. The condition (2.30) implies that there exists an elementary abelian subgroup $F \neq E_0$ of rank 2 containing Z. Since $Z = \Omega_1(Z(P))$ has order p, we have that F does not centralize E_0 and hence EF is an extraspecial p-group of type I and order p^3 by Lemma 2.4.1. Since $|P| = p^4$, it follows that E_0F is maximal in P so that the result holds for $\ell = 2$.

We suppose now $\ell \geq 3$ and we have by assumption that

$$\tilde{H}_{\ell-2}(\mathcal{A}_p(P)_{\geq 2}) \neq 0. \tag{2.31}$$

This condition (2.31) implies in particular that P is not cyclic and that P is not quaternion if $p = 2$. Since $\ell \geq 3$, this implies also that P is not dihedral, nor semi-dihedral. It follows now that P has a normal elementary abelian subgroup E_0 of rank 2 with $Z \leq E_0$. Let $M = C_P(E_0)$, we can now apply the homological version of the Bouc-Thévenaz Wedge Decomposition Formula and we obtain an isomorphism

$$\tilde{H}_0(\mathcal{A}_p(P)_{\geq 2}) \cong \bigoplus_{F \in \mathcal{F}} \tilde{H}_{-1}(\mathcal{A}_p(C_M(F))_{\geq 2}),$$

where $\mathcal{F} = \{F \in \mathcal{A}_p(P)_{\geq 2} \,|\, F \cap M = Z\}$.

Since the left-hand term is not trivial by assumption, there exists $F_0 \in \mathcal{F}$ such that $\tilde{H}_{\ell-3}(\mathcal{A}_p(C_M(F))_{\geq 2}) \neq 0$. Let us write $C_0 = C_M(F_0)$ to simplify the notations and let p^a be the order of C_0. Since C_0 is strictly contained in M we have $a \leq 2\ell - 2$. Furthermore, Lemma 2.4.2 implies $\ell - 3 < \lfloor \frac{a-1}{2} \rfloor$. These two conditions on a imply $a = 2\ell - 2$ or $a = 2\ell - 3$.

Let us see first what happens if $a = 2\ell - 2$. In this situation, C_0 is maximal in M and $P = C_0 * E_0F_0$. But since the order of C_0 is $p^{2(\ell-1)}$ and $\tilde{H}_{\ell-3}(\mathcal{A}_p(C_M(F))_{\geq 2}) \neq 0$, we have by induction that C_0 has a maximal subgroup N extraspecial of type I. The subgroup $N * E_0F_0$ is then extraspecial of type I and maximal in P.

Let us see now what happens if $a = 2\ell - 3 = 2(\ell - 2) + 1$. Since we have $\tilde{H}_{\ell-3}(\mathcal{A}_p(C_M(F))_{\geq 2}) \neq 0$, it follows by the previous Proposition 2.4.3 that C_0 is extraspecial of type I. Therefore $C_0 * E_0F_0$ is extraspecial of type I and is maximal in P.

In both cases P has a maximal subgroup extraspecial of type I and the proposition is proved. □

Example 2.4.5. Let $\ell \geq 2$.

a) If $P = (X_{p^3})^{*(\ell-1)} * C_{p^2}$, then $|P| = p^{2\ell}$ and $\tilde{H}_{\ell-2}(\mathcal{A}_p(P)_{\geq 2}) \neq 0$.

b) If $p = 2$ and $P = D_8^{*(\ell-2)} * S$, where S is either D_{16} or SD_{16}, then $|P| = 2^{2\ell}$ and $\tilde{H}_{\ell-2}(\mathcal{A}_p(P)_{\geq 2}) \neq 0$.

If P is a p-group of order $p^{2\ell}$ with a cyclic Frattini subgroup and such that $\tilde{H}_{\ell-2}(\mathcal{A}_p(P)_{\geq 2}) \neq 0$, then it follows from the classifications obtained in Chapter 1 and the calculations performed in Section 2.3, that P is one of the groups of Example 2.4.5.

To our knowledge, there is no classification of p-groups with a maximal subgroup extraspecial of type I. The two following examples show that there are however other examples than those given in Example 2.4.5.

Example 2.4.6. Let $X = X_{p^3}$ be an extraspecial p-group of type I and order p^3 and let x, y be two generators of order p of X. There is an automorphism α of X of order p, given by $\alpha(x) = x$ and $\alpha(y) = xy$. Let $A = \langle a \rangle$ be a cyclic group of order p and let $P = X \rtimes A$ be the semi-direct product of A acting on X, with respect to the homomorphism $A \to \mathrm{Aut}(X)$ sending a to α. We identify X and A with the corresponding subgroups in P and we let $z = [x, y]$. We have now that P is generated by the elements x, y and a of order p and we have the following relations:

$$\begin{aligned} [x, y] &= z; \\ axa^{-1} &= x; \\ aya^{-1} &= xy. \end{aligned}$$

Remark first that $P' = \Phi(P) = \langle x, z \rangle$, so that P does not have a cyclic Frattini subgroup. Note that $|P| = p^4 = p^{2\ell}$, with $\ell = 2$ and on the one hand, the subgroup $M = \langle z, x, a \rangle$ is elementary abelian and maximal in P. On the other hand, the subgroup $F = \langle z, y \rangle$ is elementary abelian, but is not properly contained in any elementary abelian subgroup of P. This shows that the poset $\mathcal{A}_p(P)_{\geq 2}$ is disconnected and hence $\tilde{H}_{\ell-2}(\mathcal{A}_p(P)_{\geq 2}) = \tilde{H}_0(\mathcal{A}_p(P)_{\geq 2}) \neq 0$.

Example 2.4.7. Let p be a prime and let $X = (X_{p^3})^{*p}$ be a central product of p copies of the group X_{p^3}. We choose a generator z of $Z(X)$ and symplectic generators x_i, y_i, $i = 1, \ldots, p$, of X, all of order p and such that $[x_i, y_i] = z$ for $i = 1, \ldots, p$. Let α be the automorphism of X that permutes cyclicly the generators $\{x_1, \ldots, x_p\}$ and the generators $\{y_1, \ldots, y_p\}$. More precisely, α is defined on the generators of X by

$$\begin{aligned} \alpha(x_i) &= x_{i+1}, \text{ for } i = 1, \ldots, p-1, \quad \text{and} \quad \alpha(x_p) = x_1; \\ \alpha(y_i) &= y_{i+1}, \text{ for } i = 1, \ldots, p-1, \quad \text{and} \quad \alpha(y_p) = y_1. \end{aligned}$$

Let $A = \langle a \rangle$ be a cyclic group of order p, and let P be the semi-direct product $P = X \rtimes A$ with respect to the homomorphism $A \to \mathrm{Aut}(X)$ sending a to α. We identify X and A with the corresponding subgroups in P. Note that $|P| = p^{2p+2} = p^{2\ell}$, with $\ell = p + 1$.

Let $x = x_1 \cdots x_p$ and let $E_0 = \langle x, z \rangle$. Since $[x_i, x_j] = 1$ for $i = 1, .., p$, we have $axa^{-1} = x$. Since X is extraspecial, $y_i x y_i^{-1} = zx$ for all $i = 1, \ldots, p$.

We have thus that E_0 is normal in P and furthermore $M = C_P(E_0)$ has the following generators:

$$M = \langle a, x_1, \ldots, x_p, y_1^{-1}y_2, \ldots, y_1^{-1}y_p \rangle.$$

The subgroup $F = \langle y_1, z \rangle$ is elementary abelian of rank 2 and $F \cap M = \langle z \rangle$. Furthermore, $C_M(F)$ has the following generators:

$$C_M(F) = \langle x_2, \ldots, x_p, y_1^{-1}y_2, \ldots, y_1^{-1}y_p \rangle.$$

In particular, $C_M(F)$ is extraspecial of type I and order p^{2p-1}. It follows from Lemma 2.3.15, respectively Lemma 2.3.17 when $p = 2$, that

$$\tilde{H}_{p-2}(\mathcal{A}_p(C_M(F))_{\geq 2}) \neq 0.$$

An application of the homological version of the Bouc-Thévenaz Wedge Decomposition Formula shows now that $\tilde{H}_{\ell-2}(\mathcal{A}_p(P)_{\geq 2}) = \tilde{H}_{p-1}(\mathcal{A}_p(P)_{\geq 2}) \neq 0$.

These last two examples seem to suggest that classifying all p-groups of order $p^{2\ell}$, $\ell \geq 2$, and such that $\tilde{H}_{\ell-2}(\mathcal{A}_p(P)_{\geq 2}) \neq 0$, may be a difficult task.

2.5 Cohen-Macaulay property

If P is a non-trivial p-group, it is well known that $\mathcal{A}_p(P)$ is contractible. Consequently, one cannot distinguish between p-groups by looking at the homotopy type of $\mathcal{A}_p(P)$. The homotopy Cohen-Macaulay property (hCM for short) is more accurate, since it takes all intervals into consideration. Recall that a poset $\mathcal{P}$ is hCM if $\mathcal{P}$ and the subposets $\mathcal{P}_{<p}, (p, p'), \mathcal{P}_{>p'}$ are spherical of maximal dimension. In this section, we will determine for which of the p-groups with cyclic derived p-group the poset $\mathcal{A}_p(P)$ is hCM.

Example 2.5.1. As a first example, consider an elementary abelian p-group E of rank ℓ. The poset $\mathcal{A}_p(E)$ consists then of all non-trivial subgroups of E and can be identified with the poset $T(E)$ of all non-trivial subspaces of E viewed as an $\mathbb{F}_p$-vector space. It follows from the theory of buildings and the Solomon-Tits theorem that this poset is hCM of dimension $\ell - 1$. The reader not familiar with buildings can refer to the discussion following [23, Proposition 8.6] or to [18, Proposition 3.6] for other arguments.

As a consequence, for any group G, $\mathcal{A}_p(G)_{<A} = \mathcal{A}_p(A)_{<A}$ is spherical of maximal dimension. It is also true for any interval (A, B) in $\mathcal{A}_p(G)$ since this interval is isomorphic to $\mathcal{A}_p(B/A)_{<B/A}$. We have thus the following characterization of the hCM property for posets of the form $\mathcal{A}_p(G)$.

Proposition 2.5.2. *[23, Proposition 10.1] The poset $\mathcal{A}_p(G)$ is hCM if and only if $\mathcal{A}_p(G)$ is spherical of dimension $r_p(G) - 1$ and $\mathcal{A}_p(G)_{>A}$ is spherical of dimension $r_p(G) - r_p(A) - 1$ for any $A \in \mathcal{A}_p(G)$.*

Remark 2.5.3. Note that if $G = P$ is a p-group, then $\mathcal{A}_p(G)$ is always spherical since it is contractible.

Definition 2.5.4. We will say that a group G has the hCM property if $\mathcal{A}_p(G)$ is hCM.

Remark 2.5.5. [23, Remark 10.2] Groups with the hCM property are somewhat special since then all maximal elementary abelian subgroups have the same rank.

In this section, we will restrict our attention to p-groups, but it is useful to note that the hCM property can be transferred to p-nilpotent groups.

Proposition 2.5.6 (Corollary 11.4 in [23])**.** *Let G be a p-nilpotent group with $P = G/O_{p'}(G)$. If $\mathcal{A}_p(P)$ is hCM of dimension d then $\mathcal{A}_p(G)$ is hCM of dimension d .*

Example 2.5.7. As a second example, suppose that p is odd and let $P = X_{p^{2\ell+1}}$ be an extraspecial group of type I. The poset $\mathcal{A}_p(P)_{>Z(P)}$ is equivalent to the poset of totally isotropic subspaces of $P/Z(P)$ whose associated simplicial complex is the building of a symplectic group. It follows that $\mathcal{A}_p(P)_{>Z(P)}$ is hCM of dimension $\ell - 1 = r_p(P) - 1$. This implies that $\mathcal{A}_p(P)_{>B}$ is spherical of dimension $r_p(P) - r_p(B) - 1$ for all $B \in \mathcal{A}_p(P)$ containing $Z(P)$. If $B \in \mathcal{A}_p(P)$ does not contain $Z(P)$, then $\mathcal{A}_p(P)_{>B}$ is conically contractible via

$$A \leq AZ(P) \geq BZ(P).$$

As a consequence, $\mathcal{A}_p(P)$ is hCM of dimension $\ell = \mathrm{rk}(P)$.

The argument using buildings can be avoided by a recursive argument that we would like to present now. The same argument will be used in the rest of this section for groups for which there is no natural geometry. It is first worth noticing that the required property for $\mathcal{A}_p(P)_{>B}$ is trivially satisfied for any B containing Z, once we know that $\mathcal{A}_p(P)_{>Z}$ is hCM.

Thanks to the recursive nature of the definition of the hCM property it is not always needed to compute the homotopy type of all intervals. This is the meaning of the next lemma.

Lemma 2.5.8. *Let P be a p-group and $Z = \Omega_1(Z(P))$. If $\mathcal{A}_p(P)_{>Z}$ is spherical of dimension $\mathrm{rk}(P) - \mathrm{rk}(Z) - 1$ and $\mathcal{A}_p(C_P(A))$ is hCM of dimension $\mathrm{rk}(P) - 1$ for each A minimal in $\mathcal{A}_p(P)_{>Z}$, then $\mathcal{A}_p(P)$ is hCM.*

Proof. We have to show that $\mathcal{A}_p(P)_{>B}$ is spherical of dimension $\mathrm{rk}(P) - \mathrm{rk}(B) - 1$ for each $B \in \mathcal{A}_p(P) \cup \{1\}$. Since P is a p-group, this holds for $B = 1$, so suppose $B > 1$. If Z is not contained in B, the subgroup BZ is a conjunctive element in $\mathcal{A}_p(P)_{>B}$, so that $\mathcal{A}_p(P)_{>B}$ is contractible. If $B = Z$, then it holds by one of our assumptions, so we may suppose $Z < B$.

There exists then $A \in \mathcal{A}_p(P)_{>Z}$ of rank 2 such that $Z < A \leq B$ and we have $\mathcal{A}_p(P)_{>B} = \mathcal{A}_p(C_P(A))_{>B}$. By assumption, $\mathcal{A}_p(C_P(A))$ is hCM of dimension $\mathrm{rk}(P) - 1$, so that $\mathcal{A}_p(C_P(A))_{>B}$ is spherical of dimension $\mathrm{rk}(P) - \mathrm{rk}(B) - 1$. □

We state one more useful lemma.

Lemma 2.5.9 (Proposition 10.3 in [23])**.** *If $\mathcal{A}_p(G_1)$ and $\mathcal{A}_p(G_2)$ are hCM of dimension d_1 and d_2 respectively, then $\mathcal{A}_p(G_1 \times G_2)$ is hCM of dimension $d_1 + d_2 + 1$.*

We summarize the preceding examples in the two following lemmas.

Lemma 2.5.10. *If E is an elementary abelian p-group, then $\mathcal{A}_p(E)$ is hCM.*

As we have said before, the case of extraspecial p-groups can be deduced from arguments using buildings. We will provide here an alternative proof and this should clarify the usefulness of Lemma 2.5.8.

Lemma 2.5.11 (Example 10.4 in [23])**.** *If p is odd and P is extraspecial, then $\mathcal{A}_p(P)$ is hCM.*

Proof. If $P = X_{p^{2\ell+1}}$ is extraspecial of type I, we know from our results in the preceding section that $\mathcal{A}_p(P)_{>Z(P)}$ is a wedge of spheres of maximal dimension.

Let A be minimal in $\mathcal{A}_p(P)_{>Z(P)}$. We choose a generator z of $Z(P)$ and symplectic generators $x_1, y_1, \ldots, x_\ell, y_\ell$ of P, all of order p, and such that $[x_i, y_i] = z$, for $i = 1, \ldots, \ell$. We can assume without loss of generality that $A = \langle x_1, z\rangle$, so that $C_P(A)$ has the following generators

$$C_P(A) = \langle x_1, x_2, y_2, \ldots, x_\ell, y_\ell\rangle.$$

We have in particular that $C_P(A) = \langle x_1\rangle \times Q$, where $Q = \langle x_j, y_j, j = 2, \ldots, \ell\rangle$ is isomorphic to $X_{p^{2\ell-1}}$. We have then

$$\mathcal{A}_p(P)_{>A} = \mathcal{A}_p(C_P(A)_{>A}) = \mathcal{A}_p(\langle x_1\rangle \times Q)_{>(\langle x_1\rangle\times\langle z\rangle)} \cong \mathcal{A}_p(Q)_{>Z(Q)}.$$

A recursive argument can be used to conclude that $\mathcal{A}_p(P)_{>A}$ is hCM, once we know that X_{p^3} is hCM. But this is easy to check, since $\mathcal{A}_p(X_{p^3})_{>Z(X_{p^3})}$ is a discrete poset.

A similar argument can be used for an extraspecial p-group $P = X^-_{p^{2\ell+1}}$ of type II (see [23, Example 10.4]). But this can also be seen in the following way. The group P is a central product $X_{p^{2(\ell-1)+1}} * X^-_{p^3}$, so that $\Omega_1(P)$ is isomorphic to $X_{p^{2(\ell-1)+1}} \times C_p$. It follows then from the previous case and Lemma 2.5.9 that $\mathcal{A}_p(P)$ is hCM of dimension ℓ. □

The aim of this section is to study the hCM property for a larger class of p-groups, namely those with cyclic derived subgroup. So let P be a p-group with cyclic derived subgroup. Recall that we can suppose without restriction that $\Omega_1(P) = P$. In particular, P/P' in turn is generated by elements of order p and since it is abelian, it must have exponent p. As a consequence, we have $\Phi(P) \le P'$, so that the Frattini subgroup of P is cyclic.

Suppose for a while that p is odd. Then $\Phi(P)$ is also central (see Proposition 1.3.5), hence $|P'| = p$ and since P is generated by elements of order p, this implies that P has exponent p. Therefore, P has the form $P = Q \times E$, where E is elementary abelian and Q is extraspecial of type I. The following result follows now directly from lemmas 2.5.9, 2.5.10 and 2.5.11.

Proposition 2.5.12. *Let p be an odd prime. If P is a p-group with cyclic derived subgroup, then $\mathcal{A}_p(P)$ is hCM of dimension* $\mathrm{rk}(P) - 1$.

Remark that this closes the discussion for p odd and we will focus now on the case $p = 2$. Let P be a 2-group with $\Phi(P)$ cyclic. Recall from Lemma 1.3.2 that P can then be written as $P = Q \times E$ where E is elementary abelian and Q is a 2-group with $\Phi(P)$ and $Z(P)$ cyclic. It follows from Lemma 2.5.9 and Lemma 2.5.10 that $\mathcal{A}_p(P)$ is hCM if $\mathcal{A}_p(Q)$ also is. As a consequence, we can restrict our attention to 2-groups with cyclic center and cyclic Frattini subgroup.

Thanks to the classification obtained in the previous chapter, we can make a case-by-case study of $\mathcal{A}_p(P)$ for those groups.

If $\Phi(P)$ has order 2, arguments using buildings can be used to prove the following results. We will however provide a proof for sake of completeness.

Lemma 2.5.13.

a) If $P = D_8^{*\ell}$ with $\ell \geq 1$, then $\mathcal{A}_p(P)$ is hCM of dimension ℓ.

b) If $P = D_8^{*\ell} * C_4$ with $\ell \geq 0$, then $\mathcal{A}_p(P)$ is hCM of dimension ℓ.

c) If $P = D_8^{*\ell} * Q_8$ with $\ell \geq 0$, then $\mathcal{A}_p(P)$ is hCM of dimension ℓ.

Proof. Suppose first that $P = D_8^{*\ell}$ and let $x_1, y_1, \cdots, x_\ell, y_\ell$ be symplectic generators of P all of order 2 and let $z = [x_i, y_i]$. We already know Lemma 2.3.17, that $\mathcal{A}_p(P)_{>Z(P)} \simeq \mathcal{A}_p(P)_{\geq 2}$ has the homotopy type of a wedge of spheres of dimension $\ell - 1 = \mathrm{rk}(P) - \mathrm{rk}(Z(P)) - 1$.

Following Lemma 2.5.8 it remains to show for any $A \in \mathcal{A}_p(P)_{>Z(P)}$ with $|A| = p$ that the poset $\mathcal{A}_p(C_P(A))$ is hCM of dimension ℓ. Such a subgroup A is generated by z and an element g of order 2. Without loss of generality, we may assume $g = x_1$. It is then easy to see that $C_P(A)$ is the subgroup generated by x_1 and the elements x_j, y_j for $j \neq 1$.

Therefore $C_P(A)$ is isomorphic to $C_2 \times D_8^{*(\ell-1)}$. The result for $P = D_8^{*\ell}$ follows now from an induction argument together with the use of Lemma 2.5.9.

The proof in the two other cases is very similar. When $P = D_8^{*\ell} * C_4$, we find centralizers isomorphic to $D_8^{*(\ell-1)} * C_4$. In the case $P = D_8^{*\ell} * Q_8$ we find centralizers isomorphic to $D_8^{*(\ell-1)} * Q_8$. $\square$

Remark 2.5.14. A proof of the previous result using the quadratic form on $P/Z(P)$ can be found in a paper by Das [11].

If $|\Phi(P)| > 2$, it follows from the classification theorems 1.3.26 and 1.3.37 that P is isomorphic to $E \times (D_8^{*\ell} * S)$ where E is elementary abelian, $\ell \geq 0$ and S is one of the following groups: $C_{2^{m+1}}$, $M_{2^{m+2}}$, $D_{2^{m+2}}$, $SD_{2^{m+2}}$, $Q_{2^{m+2}}$, $D^+_{2^{m+3}}$, $Q^+_{2^{m+3}}$, $D_{2^{m+2}} * C_4$, $SD_{2^{m+2}} * C_4$, $D^+_{2^{m+3}} * C_4$ with $m > 1$.

When the Frattini subgroup is central, the result follows rather easily.

Lemma 2.5.15. *If $P = D_8^{*\ell} * C_{2^{m+1}}$ with $\ell \geq 0$, then $\mathcal{A}_p(P)$ is hCM of dimension ℓ.*

Proof. Since the subgroup $\Omega_1(P)$ is isomorphic to $D_8^{*\ell} * C_4$, this follows at once from Lemma 2.5.13. $\square$

Lemma 2.5.16. *If $P = D_8^{*\ell} * M_{2^{m+2}}$ with $\ell \geq 0$ and $m > 1$, then $\mathcal{A}_p(P)$ is hCM of dimension $\ell + 1$.*

Proof. Since $\Omega_1(P)$ is isomorphic to $(D_8^{*\ell} * C_4) \times C_2$ the result follows from Lemma 2.5.13 and Lemma 2.5.9. $\square$

It remains to treat the cases of 2-groups of the form $D_8^{*\ell} * S$ where S is one of the following groups

$$D_{2^{m+2}}, SD_{2^{m+2}}, Q_{2^{m+2}}, D^+_{2^{m+3}}, Q^+_{2^{m+3}}, D_{2^{m+2}} * C_4, SD_{2^{m+2}} * C_4, D^+_{2^{m+3}} * C_4 \tag{2.32}$$

all with $m > 1$. We wish to determine for which of these groups the poset $\mathcal{A}_p(P)$ is hCM. A necessary condition is that $\mathcal{A}_p(P)_{>Z} = \mathcal{A}_p(P)_{\geq 2}$ must be spherical. As a consequence of the calculations performed in Lemma 2.3.23, we obtain immediately the following result.

Lemma 2.5.17. *If $P = D_8^{*\ell} * SD_{2^{m+1}}$ with $\ell \geq 1$ and $m > 1$, then $\mathcal{A}_p(P)$ is not hCM.*

Note however that if $\ell = 0$ in the previous lemma, i.e. $P = SD_{2^{m+2}}$ with $m > 1$, then $\mathcal{A}_p(P)$ is hCM. This follows from the fact that $\mathcal{A}_p(P)_{>Z(P)}$ has dimension 0 in this case.

Lemma 2.5.18. *If $P = SD_{2^{m+1}}$ with $m > 1$, then $\mathcal{A}_p(P)$ is hCM of dimension 1.*

For the same reason, we have the analogous result for $P = D_{2^{m+2}}$ with $m > 1$.

Lemma 2.5.19. *Let $P = D_{2^{m+2}}$ with $m \geq 1$, then $\mathcal{A}_p(P)$ is hCM of dimension 1.*

Lemma 2.5.20. *If $P = D_8^{*\ell} * D_{2^{m+2}}$ with $m > 1$ and $\ell \geq 1$, then $\mathcal{A}_p(P)$ is hCM of dimension $\ell + 1$.*

Proof. By Proposition 2.5.8 and Lemma 2.3.21, it is enough to check that $\mathcal{A}_p(C_P(A))$ is hCM of dimension $\ell + 1$ for all A minimal in $\mathcal{A}_p(P)_{>Z}$. Let z be a generator of $Z(P)$ and let $x_1, y_1, \ldots, x_\ell, y_\ell$ be symplectic generators of the subgroup $D_8^{*\ell}$, all of order 2 and such that $[x_i, y_i] = z$. Let u, a be generators of the subgroup $D_{2^{m+2}}$ with u of order 2^{m+1}, a of order 2 and $aua^{-1} = u^{-1}$. We set furthermore $w = u^{2^m}$, so that in particular $z = w^2$.

A minimal subgroup in $\mathcal{A}_p(P)_{>Z(P)}$ is generated by z and an element $g \in P$ of order 2 which can be written $g = xs$, with x in the subgroup $D_8^{*\ell}$ and $s \in D_{2^{m+2}}$. Since $g^2 = 1$, we have $x^2 = 1 = s^2$ or $x^2 = z = s^2$.

Suppose first that x has order 2. Without loss of generality, we may assume $x = x_1$. If $s = 1$, the centralizer of A in P is generated by all the above generators of P except y_1, that is

$$C_P(A) = \langle x_1, x_2, y_2, \cdots, x_\ell, y_\ell, u, a \rangle.$$

It follows that $C_P(A)$ is isomorphic to $C_2 \times \left(D_8^{*\ell-1} * D_{2^{m+2}}\right)$. By an induction argument, this group is hCM of dimension $1 + ((\ell - 1) + 1) = \ell + 1 = \mathrm{rk}(P) - 1$.

If $s = a$, then $C_P(A)$ is generated by $x_1 a$, a, $y_1 w$ and the elements x_j, y_j with $j \neq 1$. If $x = 1$, then s has order 2 and without loss of generality we may assume $s = a$, i.e. $g = v$. In this case, $C_P(A)$ is generated by a and all elements x_i, y_i for $i = 1, \ldots, \ell$. Suppose now that x has order 4. In this case, s has also order 4 and we may suppose without loss of generality that $x = x_1 y_1$ and $s = w$, i.e. $g = x_1 y_1 w$. In this case, we find that $C_P(A)$ is generated by

g, x_1a, y_1a and the elements x_j, y_j for $j \neq 1$. In these three last cases, we see that $C_P(A)$ is isomorphic to $C_2 \times D_8^{*\ell}$, so that $\mathcal{A}_p(C_P(A))$ is hCM of dimension $\ell + 1 = \mathrm{rk}(P) - 1$ by Lemma 2.5.13. □

Lemma 2.5.21. *If $P = Q_{2^{m+2}}$ with $m > 1$, then $\mathcal{A}_p(P)$ is hCM of dimension* 0.

Lemma 2.5.22. *Let $P = D_8^{*\ell} * Q_{2^{m+2}}$ with $\ell \geq 1$ and $m > 1$. Then $\mathcal{A}_p(P)$ is hCM of dimension ℓ.*

Proof. Let u, b be generators of the subgroup $Q_{2^{m+2}}$ with u of order 2^{m+1}, b of order 4 and $bub^{-1} = u^{-1}$. Let $w = u^{2^m}$ and $z = w^2$. Let $x_1, y_1, \ldots, x_\ell, y_\ell$ be symplectic generators of the subgroup $D_8^{*\ell}$, all of order 2 and such that $[x_i, y_i] = z$. A minimal subgroup A in $\mathcal{A}_p(P)_{>Z(P)}$ is generated by z and an element $g = xs$ with x in the subgroup D_8^{*l} and s in the subgroup $Q_{2^{m+2}}$. Since $g^2 = 1$ we have that s has order at most 4. All cases can be reduced to one of the following.

If $g = x_1$, then $C_P(A)$ is generated by $x_1, x_2, y_2, \ldots, x_\ell, y_\ell$ and the subgroup $Q_{2^{m+2}}$ so that $C_P(A)$ is isomorphic to $C_2 \times \left(D_8^{*(\ell-1)} * Q_{2^{m+2}}\right)$.

If $g = x_1y_1w$, then $C_P(A)$ is generated by the following elements

$$\begin{gathered} x_j, y_j, \text{ for } j > 1, \\ x_1b, u, \\ x_1y_1w. \end{gathered}$$

It follows that $C_P(A)$ is isomorphic to $(D_8^{*(\ell-1)} * Q_{2^{m+2}}) \times C_2$.

If $g = x_1y_1b$, then $C_P(A)$ is generated by x_1y_1b, x_1w, b and the elements x_j, y_j for $j \neq 1$. It follows that $C_P(A)$ is isomorphic to $C_2 \times (D_8^{*(\ell-1)} * Q_8)$.

In all these cases, the poset $\mathcal{A}_p(C_P(A))$ is hCM of dimension ℓ by an induction argument and lemmas 2.5.13 and 2.5.21. □

Lemma 2.5.23. *If $P = D_{2^{m+2}} * C_4$ with $m > 1$, then $\mathcal{A}_p(P)$ is hCM of dimension* 1.

Proof. The poset $\mathcal{A}_p(P)_{>Z(P)}$ is a discrete poset, hence $\mathcal{A}_p(C_P(A)) = A$ is hCM of dimension $\mathrm{rk}(P) - 1$, for any $A \in \mathcal{A}_p(P)_{>Z(P)}$. □

The proofs for $P = D_8^{*\ell} * D_{2^{m+2}} * C_4$ and $P = D_8^{*\ell} * SD_{2^{m+2}} * C_4$ are very similar so that we will not write them both. We have chosen to write the proof for $P = D_8^{*\ell} * SD_{2^{m+2}} * C_4$ for the following reason. We have seen previously that the group $P = D_8^{*\ell} * SD_{2^{m+2}}$ is not hCM whereas the group $P = D_8^{*\ell} * SD_{2^{m+2}} * C_4$ is hCM. The reason for this difference will precisely appear in the proof.

Lemma 2.5.24. *Let $P = D_8^{*\ell} * D_{2^{m+2}} * C_4$ with $\ell \geq 1$ and $m > 1$. Then $\mathcal{A}_p(P)$ is hCM of dimension $\ell + 1$.*

Lemma 2.5.25. *If $P = SD_{2^{m+2}} * C_4$ with $m > 1$, then $\mathcal{A}_p(P)$ is hCM of dimension* 1.

Proof. The poset $\mathcal{A}_p(P)_{>Z(P)}$ is a discrete poset, hence $\mathcal{A}_p(C_P(A)) = A$ is hCM of dimension $\mathrm{rk}(P) - 1$, for any $A \in \mathcal{A}_p(P)_{>Z(P)}$. □

Lemma 2.5.26. *Let $P = D_8^{*\ell} * SD_{2^{m+2}} * C_4$ with $\ell \geq 1$ and $m > 1$. Then $\mathcal{A}_p(P)$ is hCM of dimension $\ell + 1$.*

Proof. Let c be a generator of the subgroup C_4 and let u, a be generators of the subgroup $SD_{2^{m+2}}$ with u of order 2^{m+1}, a of order 2 and $aua^{-1} = u^{-1+2^m}$. Let $w = u^{2^{m-1}}$ and $z = w^2 = c^2$. Let $x_1, y_1, \ldots, x_\ell, y_\ell$ be symplectic generators of the subgroup $D_8^{*\ell}$, all of order 2 and such that $[x_i, y_i] = z$. A minimal subgroup A in $\mathcal{A}_p(P)_{>Z(P)}$ is generated by z and an element $g = xs$ with x in the subgroup D_8^{*l} and s in the subgroup $SD_{2^{m+2}} * C_4$. All cases can be reduced to one of the following.

If $g = a$, then $C_P(A)$ is generated by the subgroup $D_8^{*\ell}$ and the two elements c and a, so that $C_P(A)$ is isomorphic to $(D_8^{*\ell} * C_4) \times C_2$.

If $g = wc$, then $C_P(A)$ is generated by the subgroup $D_8^{*\ell}$ and the two elements u and wc, so that $C_P(A)$ is isomorphic to $(D_8^{*\ell} * C_{2^{m+1}}) \times C_2$.

If $g = auc$, then $C_P(A)$ is generated by the subgroup $D_8^{*\ell}$ and the two elements c and auc, so that $C_P(A)$ is isomorphic to $(D_8^{*\ell} * C_4) \times C_2$.

If $g = x_1$, then $C_P(A)$ is generated by $x_1, x_2, y_2, \ldots, x_\ell, y_\ell$ and the subgroup $SD_{2^{m+2}} * C_4$ so that $C_P(A)$ is isomorphic to $C_2 \times (D_8^{*(\ell-1)} * SD_{2^{m+2}} * C_4)$.

If $g = x_1 a$, then $C_P(A)$ is generated by $x_1 a$, $y_1 wc$, c and the elements x_j, y_j for $j \neq 1$. It follows that $C_P(A)$ is isomorphic to $(D_8^{*(\ell-1)} * C_4) \times C_2 \times C_2$.

If $g = x_1 wc$, then $C_P(A)$ is generated by $x_1 wc$, $y_1 a$, c and the elements x_j, y_j for $j \neq 1$. It follows that $C_P(A)$ is isomorphic to $(D_8^{*(\ell-1)} * C_4) \times C_2 \times C_2$.

If $g = x_1 auc$, then $C_P(A)$ is generated by $x_1 auc$, $y_1 wc$, c and the elements x_j, y_j for $j \neq 1$. It follows that $C_P(A)$ is isomorphic to $(D_8^{*(\ell-1)} * C_4) \times C_2 \times C_2$.

If $g = x_1 y_1 w$, then $C_P(A)$ is generated by $x_1 y_1 w$, $y_1 a$, u, c and the elements x_j, y_j for $j \neq 1$. It follows that $C_P(A)$ is isomorphic to $(D_8^{*(\ell-1)} * SD_{2^{m+2}}) \times C_2$.

If $g = x_1 y_1 au$, then $C_P(A)$ is generated by $x_1 y_1 au$, $x_1 w$, $y_1 wc$, c and the elements x_j, y_j for $j \neq 1$. It follows that $C_P(A)$ is isomorphic to the group $(D_8^{*(\ell-1)} * D_8 * C_4) \times C_2$. Note that this is, in some sense, the crucial case as the next remark will show.

If $g = x_1 y_1 ac$, then $C_P(A)$ is generated by $x_1 y_1 ac$, $x_1 w$, $y_1 wc$, c and the elements x_j, y_j for $j \neq 1$. It follows that $C_P(A)$ is isomorphic to the group $(D_8^{*(\ell-1)} * D_8 * C_4) \times C_2$.

If $g = x_1 y_1 c$, then $C_P(A)$ is generated by $x_1 y_1 c$, u, a, c and the elements x_j, y_j for $j \neq 1$. It follows in this case that $C_P(A)$ is isomorphic to the group $(D_8^{*(\ell-1)} * SD_{2^{m+2}} * C_4) \times C_2$.

In all these cases, the poset $\mathcal{A}_p(C_P(A))$ is hCM of dimension $\ell + 1$ by an induction argument and our previous results, especially lemmas 2.5.9 and 2.5.15. □

Remark 2.5.27. The crucial case in the preceding proof is when $g = x_1 y_1 au$. In this situation, we obtained $C_P(A) = (D_8^{*(\ell-1)} * D_8 * C_4) \times C_2$. The subgroup $D_8 * C_4$ is generated by $y_1 w, x_1 wc$ and c.

There is an analogous situation for the group $Q = D_8^{*\ell} * SD_{2^{m+2}}$, but for this group, $C_Q(A)$ would be isomorphic to $D_8^{*\ell-1} * Q_8$, which has not the required dimension. This is roughly why $\mathcal{A}_p(Q)$ is not hCM. The subgroup Q_8 would be here generated by the two elements x_1w and y_1w, of order 4.

Because of the presence of the central element c of order 4, when P is the group $D_8^{*\ell} * SD_{2^{m+2}} * C_4$, the two elements x_1w and y_1w, of order 4, can be modified by c in order to change their order. This is the well-known isomorphism $Q_8 * C_4 \cong D_8 * C_4$. In this situation, the centralizer has the required dimension allowing $\mathcal{A}_p(P)$ to be hCM, when $P = D_8^{*\ell} * SD_{2^{m+2}} * C_4$.

Lemma 2.5.28. *If $P = D_8^{*\ell} * D^+_{2^{m+3}}$ with $\ell \geq 0$ and $m > 1$, then $\mathcal{A}_p(P)$ is not hCM.*

Proof. By Remark 2.5.5, it is enough to exhibit two subgroups that are maximal in $\mathcal{A}_p(P)$ but that do not have the same rank. Let z be a generator of $Z(P)$. Let $x_1, y_1, \dots, x_\ell, y_\ell$ be symplectic generators of $D_8^{*\ell}$ all of order 2 and such that $[x_i, y_i] = z$. Let a, b, u be generators of $D^+_{2^{m+3}}$ with a and b of order 2, u of order 2^{m+1}, $aua^{-1} = u^{1+2^m}$ and $bub^{-1} = u^{-1}$. On the one hand, the subgroup $\langle z, x_1, \dots, x_\ell, a, b\rangle$ is maximal in $\mathcal{A}_p(P)$ and has rank $\ell + 3$. On the other hand, the subgroup $\langle z, x_1, \dots, x_\ell, ub\rangle$ is also maximal in $\mathcal{A}_p(P)$ but has rank $\ell + 2$. □

Lemma 2.5.29. *If $P = Q^+_{2^{m+3}}$ with $m > 1$, then $\mathcal{A}_p(P)$ is hCM of dimension 1.*

Proof. Let a, b, u be generators of $Q^+_{2^{m+3}}$ with a of order 2, b of order 4, u of order 2^{m+1}, $aua^{-1} = u^{1+2^m}$ and $bub^{-1} = u^{-1}$. We have seen in Lemma 2.3.24, that $\mathcal{A}_p(P)_{>Z(P)}$ is a discrete poset and it follows that $\mathcal{A}_p(P)$ is hCM. □

Lemma 2.5.30. *Let $P = D_8^{*\ell} * Q^+_{2^{m+3}}$ with $\ell \geq 1$ and $m > 1$. Then $\mathcal{A}_p(P)$ is hCM of dimension $\ell + 1$.*

Proof. Let a, b, u be generators of $Q^+_{2^{m+3}}$ with a of order 2, b of order 4, u of order 2^{m+1}, $aua^{-1} = u^{1+2^m}$ and $bub^{-1} = u^{-1}$. Let $w = u^{2^{m-1}}$ and let $x_1, y_1, \dots, x_\ell, y_\ell$ be symplectic generators of $D_8^{*\ell}$ all of order 2 and such that $[x_i, y_i] = z$. Let $Z = \langle z\rangle$ and let $A = \langle z, g\rangle \in \mathcal{A}_p(P)_{>Z}$.

If $g = a$, then $C_P(A)$ is generated by all the elements x_i, y_i, $i = 1, \dots, \ell$, and the elements b, u^2 and a. It follows that $C_P(A)$ is isomorphic to the group $(D_8^{*\ell} * D_{2^{m+1}}) \times C_2$.

If $g = x_1a$, then $C_P(A)$ is generated by the elements x_j, y_j with $j \neq 1$, and the elements a, b, y_1u and x_1a. It follows that $C_P(A)$ is isomorphic to $(D_8^{*\ell-1} * Q^+_{2^{m+3}}) \times C_2$.

If $g = abu$, then $C_P(A)$ is generated by all the elements x_i, y_i, $i = 1, \dots, \ell$, and the elements wa and abu. It follows that $C_P(A)$ is isomorphic to the group $(D_8^{*\ell} * C_4) \times C_2$.

If $g = x_1abu$, then $C_P(A)$ is generated by the elements x_j, y_j with $i \neq 1$, and the elements x_1, y_1a, aw and abu. It follows that $C_P(A)$ is isomorphic to $(D_8^{*\ell} * C_4) \times C_2$.

If $g = x_1y_1w$, then $C_P(A)$ is generated by the elements x_j, y_j with $j \neq 1$, and the elements a, y_1b, u and x_1y_1w. It follows that $C_P(A)$ is isomorphic to $(D_8^{*\ell-1} * Q^+_{2^{m+3}}) \times C_2$.

If $g = x_1y_1b$, then $C_P(A)$ is generated by the elements x_j, y_j with $j \neq 1$, and the elements b, w, a and x_1y_1b. It follows that $C_P(A)$ is isomorphic to $(D_8^{*(\ell-1)} * Q_8) \times C_2 \times C_2$.

If $g = x_1y_1bu$, then $C_P(A)$ is generated by the elements x_j, y_j with $j \neq 1$, and the elements x_1a, y_1a, aw and x_1y_1bu. It follows that $C_P(A)$ is isomorphic to $(D_8^{*\ell} * C_4) \times C_2$.

If $g = x_1y_1bu^2$, then $C_P(A)$ is generated by the elements x_j, y_j with $j \neq 1$, and the elements x_1w, y_1w, a and x_1y_1bu. It follows that $C_P(A)$ is isomorphic to $(D_8^{*(\ell-1)} * Q_8) \times C_2 \times C_2$.

If $g = x_1y_1abu^2$, then $C_P(A)$ is generated by the elements x_j, y_j with $j \neq 1$, and the elements x_1w, y_1w, a and $x_1y_1abu^2$. It follows that $C_P(A)$ is isomorphic to $(D_8^{*(\ell-1)} * Q_8) \times C_2 \times C_2$.

In all these cases, it follows by induction and our previous results, especially lemmas 2.5.9, 2.5.13, 2.5.20, that $\mathcal{A}_p(C_P(A))$ is hCM of dimension $\ell + 1$. □

Lemma 2.5.31. *If $P = D^+_{2^{m+3}} * C_4$ with $m > 1$, then $\mathcal{A}_p(P)$ is hCM of dimension 2.*

Proof. Let z be a generator of $Z(P)$ and let c be a generator of C_4 such that $c^2 = z$. Let u, a, b be generators of $D^+_{2^{m+3}}$ with a, b of order 2, u of order 2^{m+1}, $aua^{-1} = u^{1+2^m}$ and $bub^{-1} = u^{-1}$. Set furthermore $w = u^{2^{m-1}}$.

Let $A = \langle z, g\rangle$ be a minimal element in $\mathcal{A}_p(P)_{>Z}$. We have to show that $\mathcal{A}_p(C_P(A))$ is hCM. If $g = u^ia^jb^kc^l$ with $k = 1$, then $C_P(A)$ is generated by g, c and either awc if i is odd, or a if i is even. In both cases $C_P(A)$ is isomorphic to $C_2 \times C_2 \times C_4$ so that $\mathcal{A}_p(C_P(A))$ is hCM of dimension 2.

If $g = a$, then $C_P(A)$ is generated by b, u^2, c and a, so that $C_P(A)$ isomorphic to $(D_{2^{m+1}} * C_4) \times C_2$. Hence $\mathcal{A}_p(C_P(A))$ is hCM of dimension 2.

If $g = wc$ then $C_P(A)$ is generated by a, u and wc, so that $C_P(A)$ is isomorphic to $M_{2^{m+2}} \times C_2$ and thus $\mathcal{A}_p(C_P(A))$ is hCM of dimension 2.

If $g = wac$, then $C_P(A)$ is generated by bu, u^2, c and h so that $C_P(A)$ is isomorphic to $(D_{2^{m+1}} * C_4) \times C_2$ and thus $\mathcal{A}_p(C_P(A))$ is hCM of dimension 2. □

Proposition 2.5.32. *If $P = D_8^{*\ell} * D^+_{2^{m+3}} * C_4$ with $\ell \geq 1$ and $m > 1$, then $\mathcal{A}_p(P)$ is hCM of dimension $\ell + 2$.*

Proof. Let z be a generator of $Z(P)$. Let $x_1, y_1, \dots, x_\ell, y_\ell$ be symplectic generators of $D_8^{*\ell}$ all of order 2 and with $[x_i, y_i] = z$. Let u, a, b be generators of $D^+_{2^{m+3}}$ with u of order 2^{m+1}, a, b of order 2, $aua^{-1} = u^{1+2^m}$ and $bub^{-1} = u^{-1}$. Let c be a generator of C_4 and let $w = u^{2^{m-1}}$.

Let $A = \langle z, g\rangle$ be minimal in $\mathcal{A}_p(P)_{>Z}$, we have to show that $\mathcal{A}_p(C_P(A))$ is hCM of dimension $\ell+2$. We can write $g = xs$ with $x \in D_8^{*\ell}$ and $s \in D^+_{2^{m+3}} * C_4$.

If $g = xu^ia^jb^kc^l$ with $u^i \notin \langle w\rangle$, then $C_P(A)$ is isomorphic to the group $(D_8^{*n} * C_4) \times C_2 \times C_2$, so that $\mathcal{A}_p(C_P(A))$ is hCM of dimension $\ell + 2$ by results obtained previously.

If $g = xw^ia^jb^kc^l$, then $C_P(A)$ is isomorphic to $(D_8^{*\ell-1} * D_{2^{m+3}} * C_4) \times C_2$, so that by induction $\mathcal{A}_p(C_P(A))$ is hCM of dimension $((\ell-1)+2)+1 = \ell+2$. □

The above results are summarized in Table 2.2 located on page 88.

P	hCM and dimension
$X_{p^{2\ell+1}}$	hCM of dimension ℓ
$X_{p^{2(\ell-1)+1}} * X^-_{p^3}$	hCM of dimension ℓ
$X_{p^{2\ell+1}} * C_{p^m}$	hCM of dimension ℓ
$X_{p^{2(\ell-1)+1}} * M_{p^{m+2}}$	hCM of dimension ℓ
$D_8^{*\ell}$	hCM of dimension ℓ
$D_8^{*\ell} * C_4$	hCM of dimension ℓ
$D_8^{*(\ell-1)} * Q_8$	hCM of dimension $\ell - 1$
$D_8^{*\ell} * C_{2^{m+1}}$	hCM of dimension ℓ
$D_8^{*(\ell-1)} * M_{2^{m+2}}$	hCM of dimension ℓ
$D_8^{*(\ell-1)} * D_{2^{m+2}}$	hCM of dimension ℓ
$SD_{2^{m+3}}$	hCM of dimension 1
$D_8^{*\ell} * SD_{2^{m+1}}$	not hCM
$D_8^{*(\ell-1)} * Q_{2^{m+2}}$	hCM of dimension $\ell - 1$
$D_8^{*(\ell-1)} * D_{2^{m+2}} * C_4$	hCM of dimension ℓ
$D_8^{*(\ell-1)} * SD_{2^{m+2}} * C_4$	hCM of dimension ℓ
$D_8^{*(\ell-1)} * D^+_{2^{m+3}}$	not hCM
$D_8^{*(\ell-1)} * Q^+_{2^{m+3}}$	hCM of dimension ℓ
$D_8^{*(\ell-1)} * D^+_{2^{m+3}} * C_4$	hCM of dimension $\ell + 1$

Table 2.2: hCM property for $\mathcal{A}_p(P)$ for some p-groups. In this table, $\ell \geq 1$ and $m > 1$

2.6 Homology with non-constant coefficients

Definitions

Let $f : \mathcal{P} \to \mathcal{Q}$ be a poset map. If the poset $\mathcal{Q}$ and the fibers $f^{-1}_{\leq q}$ are "sufficiently well-behaved", the homology groups of $\mathcal{P}$ can be computed using the following spectral sequence introduced by Quillen in [23]:

$$E^2_{rs} = H_r(\mathcal{Q}, q \mapsto H_s(f^{-1}_{\leq q})) \Rightarrow H_{r+s}(\mathcal{P}) \tag{2.33}$$

Quillen used it to show that certain properties of $\mathcal{Q}$ can be transferred to $\mathcal{P}$. He used it for example to prove Proposition 7.6 in [23] that asserts that if $f^{-1}_{\leq q}$ is n-connected for each $q \in \mathcal{Q}$ then $\mathcal{P}$ is n-connected if $\mathcal{Q}$ is.

It is important to note that the homology groups occurring in the E^2-terms of the spectral sequence (2.33) are not usual homology groups. As the notation $q \mapsto H_s(f^{-1}_{\leq q})$ suggests, the coefficients are not given by a constant abelian group. In this section we will recall the definition of homology groups with non-constant coefficients and we will derive a spectral sequence that may be used to compute such homology groups in term of standard homology groups.

Recall that any poset $\mathcal{P}$ can be viewed as a category with a unique morphism $x \to x'$ if $x < x'$. In particular, we can consider the category of functors from $\mathcal{P}$ with values in the category Ab of abelian groups. If $F : \mathcal{P} \to Ab$ is such a functor, then for $x < x'$ we denote $F_{x,x'} : F(x) \to F(x')$ the image of the unique map $x \to x'$. If $F : \mathcal{P} \to Ab$ is a functor and $\sigma = (x_0 < \ldots < x_k)$ is a k-simplex, we let $F(\sigma) = F(x_0)$.

Let $\mathcal{P}$ be a poset and $F : \mathcal{P} \to Ab$ be a functor. For $k \geq 0$, we define $(C_k(\mathcal{P}, F), \delta)$ to be the abelian group given by

$$C_k(\mathcal{P}, F) = \bigoplus_{\sigma \in C_k(\mathcal{P})} F(\sigma)$$

By convention, we set $C_{-1}(\mathcal{P}, F) = 0$. For any k-simplex $\sigma = (x_0 < \ldots < x_k)$ and $\lambda \in F(\sigma)$, we denote by $\lambda \cdot \sigma$ the element of $C_k(\mathcal{P}, F)$ with value λ in the component corresponding to σ and 0 otherwise.

We define the differential δ on $C_*(\mathcal{P}, F)$ in the following way. For any $\lambda \cdot \sigma$ in $C_k(\mathcal{P}, F)$, with $\sigma = (x_0 < \cdots < x_k)$ and $\lambda \in F(\sigma)$, let

$$\delta(\lambda \cdot \sigma) = F_{x_0,x_1}(\lambda) \cdot d_0(\sigma) + \sum_{i=1}^{k} (-1)^i \lambda \cdot d_i(\sigma)$$

where d_i is the usual differential.

Definition 2.6.1. For $k \geq 0$, we define the homology groups $H_k(\mathcal{P}, F)$ of $\mathcal{P}$ with coefficients in the functor F to be the homology groups of the complex $(C_*(\mathcal{P}, F), \delta)$.

Filtration of the coefficients and spectral sequence

In what follows, $\mathcal{P}$ is an arbitrary poset and F is a functor from $\mathcal{P}$ to Ab. We show that the homology groups with non-constant coefficients can be computed in terms of homology groups with constant coefficients using a spectral sequence.

For an abelian group A, we denote $\underline{A} : \mathcal{P} \to Ab$ the constant functor sending each element $y \in \mathcal{P}$ to the abelian group A. For $y < y'$ in $\mathcal{P}$, the image under $\underline{A}$ of the unique map $y \to y'$ is the identity map on A.

For an abelian group A and $y \in \mathcal{P}$, we define the functor $A_{(y)}$ as the functor sending y to A and any element $y' \in \mathcal{P}$ with $y' \neq y$ to 0.

The truncation at height k of a functor $F : \mathcal{P} \to Ab$ is the functor $F_{\leq k}$ defined by

$$F_{\leq k}(y) = \begin{cases} F(y) & \text{if } h(y) \leq k \\ 0 & \text{otherwise} \end{cases}$$

and for $y < y'$, the map $F_{\leq k}(y) \to F_{\leq k}(y')$ is the map $F(y) \to F(y')$ if $h(y') \leq k$ and zero otherwise. In a similar way, we define the functor F_k

$$F_k(y) = \begin{cases} F(y) & \text{if } h(y) = k \\ 0 & \text{else} \end{cases}$$

We will also use the conventions $F_{\leq -1} = F_{-1} = 0$.

Lemma 2.6.2. *The functor F_k is the direct sum of the functors $F(y)_{(y)}$, where y ranges over all elements of height k in $\mathcal{P}$.*

Lemma 2.6.3. *For $k \geq 0$, the transformation $t_k : F_{\leq k} \to F_{\leq k-1}$, defined as the identity on $F(y)$ if $h(y) \leq k-1$ and 0 otherwise, is a natural transformation between the functors $F_{\leq k}$ and $F_{\leq k-1}$.*

Proof. We have to check that whenever $y < y'$ the following square commutes:

$$\begin{tikzcd} F_{\leq k}(y) \arrow[r] \arrow[d] & F_{\leq k-1}(y) \arrow[d] \\ F_{\leq k}(y') \arrow[r] & F_{\leq k-1}(y') \end{tikzcd} \tag{2.34}$$

This is clear if $k = 0$, since then the two right-hand terms are 0. We suppose from now on that $k \geq 1$. If $h(y') > k$, then 2.34 commutes, since then both $F_{\leq k}$ and $F_{\leq k-1}$ have value 0 on y'. If $h(y') = k$, then $h(y) \leq k-1$ and (2.34) becomes

$$\begin{tikzcd} F(y) \arrow[r] \arrow[d] & F(y) \arrow[d] \\ F(y') \arrow[r] & 0 \end{tikzcd}$$

If $h(y') \leq k-1$, then (2.34) becomes

$$\begin{tikzcd} F(y) \arrow[r] \arrow[d] & F(y) \arrow[d] \\ F(y') \arrow[r] & F(y') \end{tikzcd}$$

where both horizontal maps are the identity and both vertical maps are the map $F_{y,y'}$. Therefore the square commutes. ∎

In a similar way, we can define a natural transformation $F_k \to F_{\leq k}$ as the identity on $F(y)$ when $h(y) = k$ and 0 otherwise. The verifications are similar to those in the previous lemma.

Lemma 2.6.4. *For $k \geq 0$, there is a short exact sequence of functors*

$$0 \to F_k \to F_{\leq k} \to F_{\leq k-1} \to 0$$

Proof. We have to show that for each $y \in \mathcal{P}$ the following sequence is exact.

$$0 \to F_k(y) \to F_{\leq k}(y) \to F_{\leq k-1}(y) \to 0.$$

If $k = 0$, then this sequence is exact since $F_0 = F_{\leq 0}$ and $F_{-1} = 0$. Suppose now that $k \geq 1$. If $h(y) > k$, the sequence is clearly exact since in this situation $F_k(y) = F_{\leq k}(y) = F_{\leq k-1}(y) = 0$. If $h(y) = k$, then the sequence becomes

$$0 \to F(y) \to F(y) \to 0 \to 0.$$

If $h(y) \leq k - 1$, then the sequence becomes

$$0 \to 0 \to F(y) \to F(y) \to 0.$$

These two sequences are exact since in both cases the map $F(y) \to F(y)$ is the identity and the lemma is proved. □

Let d be such that $F(y) = 0$ if $h(y) > d$. Such a d always exists and we can take for example $d = \dim(\mathcal{P})$. We have a sequence of natural transformations

$$F = F_{\leq d} \to F_{\leq d-1} \to \cdots \to F_{\leq 1} \to F_{\leq 0} \to 0.$$

Let K_m be the functor defined as the kernel of the map $F \to F_{\leq d-m}$. This gives a filtration of F

$$0 = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_d \subseteq K_{d+1} = F. \tag{2.35}$$

Furthermore, the successive quotients are given by $K_{i+1}/K_i \cong F_{d-i}$. This follows from the following general result.

Lemma 2.6.5. *Let $A \xrightarrow{f} B \xrightarrow{g} C$ be homomorphisms between abelian groups such that* $\ker g \subseteq \operatorname{Im} f$. *Then* $\ker g \cong \ker(gf)/\ker f$.

The filtration (2.35) of F induces in turn a filtration of the complex $C_*(\mathcal{P}, F)$. We obtain therefore a spectral sequence converging to the homology of $C_*(\mathcal{P}, F)$.

Proposition 2.6.6. *Let $\mathcal{P}$ be a poset, $F : \mathcal{P} \to Ab$ a functor and let d such that $h(y) > d$ implies $F(y) = 0$. There is a spectral sequence*

$$E^1_{rs} = H_{r+s}(\mathcal{P}, F_{d-r}) \Rightarrow H_{r+s}(\mathcal{P}, F) \tag{2.36}$$

As we have remarked earlier, the functors F_k are direct sums of functors of the form $F(y)_{(y)}$. The homology with such functors $F(y)_{(y)}$ as coefficients can be expressed in term of standard homology groups thanks to the following lemma due to Quillen [23, (9.5)].

Lemma 2.6.7. *Let A be an abelian group and let $r \geq 0$. There is an isomorphism*
$$H_r(\mathcal{P}, A_{(y)}) \cong \tilde{H}_{r-1}(\mathcal{P}_{>y}, A).$$

Proof. See (9.5) in [23]. □

Lemma 2.6.8. *Let $\mathcal{P}$ be a poset and $F : \mathcal{P} \to Ab$ a functor. There is an isomorphism*
$$H_r(\mathcal{P}, F_k) \cong \bigoplus_{\substack{y \in \mathcal{P} \\ h(y)=k}} \tilde{H}_{r-1}(\mathcal{P}_{>y}, F(y))$$

Proof. The functor F_k is the direct sum of the functors $F(y)_{(y)}$ where y ranges over the elements of height k in $\mathcal{P}$. It follows that
$$H_r(\mathcal{P}, F_k) \cong H_r(\mathcal{P}, \bigoplus_{h(y)=k} F(y)_{(y)}) \cong \bigoplus_{h(y)=k} H_r(\mathcal{P}, F(y)_{(y)}).$$

Lemma 2.6.7 implies now that $H_r(\mathcal{P}, F(y)_{(y)})$ is isomorphic to $\tilde{H}_{r-1}(P_{>y}, F(y))$ and the lemma is proved. □

Putting everything together, we obtain the following spectral sequence to compute homology groups with non-constant coefficients.

Proposition 2.6.9. *Let $F : \mathcal{P} \to Ab$ be a functor and let d be such that $F(y) = 0$ if $h(y) > d$. There is a spectral sequence*
$$E^1_{rs} = \bigoplus_{\substack{y \in \mathcal{P} \\ h(y)=d-r}} \tilde{H}_{r+s-1}(\mathcal{P}_{>y}, F(y)) \Rightarrow H_{r+s}(\mathcal{P}, F) \qquad (2.37)$$

2.7 A spectral sequence for upper intervals

Quillen's spectral sequence

To any poset map $f : \mathcal{P} \to \mathcal{Q}$ is associated a functor $\mathcal{Q} \to Ab$ defined by $q \mapsto H_s(f^{-1}_{\leq q})$.

Proposition 2.7.1 (Quillen)**.** *Let $f : \mathcal{P} \to \mathcal{Q}$ be a poset map, there is a spectral sequence*
$$E^2_{rs} = H_r(\mathcal{Q}, q \mapsto H_s(f^{-1}_{\leq q})) \Rightarrow H_{r+s}(\mathcal{P})$$

Proof. See (7.7) in [23]. □

In what follows we will assume that $f : \mathcal{P} \to \mathcal{Q}$ is a poset map such that

1. $\mathcal{Q}$ is contractible,
2. for any $y \in \mathcal{Q}$, the fiber $f^{-1}_{\leq q}$ has the homotopy type of a wedge of spheres of dimension 0.

As a first consequence, we have $H_s(f^{-1}_{\leq q}) = 0$ for all $s > 0$ and this yields the following lemma.

Lemma 2.7.2. *For $s \geq 1$, $E^2_{rs} = 0$. Furthermore $E^\infty_{rs} = E^2_{rs}$ and for any $r \geq 0$ we have $H_r(\mathcal{P}) \cong E^2_{r,0}$.*

Lemma 2.7.3. *We have $E^2_{r0} \cong H_r(\mathcal{Q}, q \mapsto \tilde{H}_0(f^{-1}_{\leq q}))$ for $r > 1$ and a short exact sequence*

$$0 \to H_0(\mathcal{Q}, q \mapsto \tilde{H}_0(f^{-1}_{\leq q})) \to E^2_{00} \to \mathbb{Z} \to 0 \tag{2.38}$$

corresponding to the short exact sequence

$$0 \to H_0(\mathcal{Q}, q \mapsto \tilde{H}_0(f^{-1}_{\leq q})) \to H_0(\mathcal{Q}, q \mapsto H_0(f^{-1}_{\leq q})) \to H_0(\mathcal{Q}, \mathbb{Z}) \to 0$$

Proof. Let $\underline{\mathbb{Z}} : \mathcal{Q} \to Ab$ denote the constant functor sending each element $q \in \mathcal{Q}$ to $\mathbb{Z}$. The short exact sequence of functors

$$0 \to \Big(q \mapsto \tilde{H}_0(f^{-1}_{\leq q})\Big) \to \Big(q \mapsto H_0(f^{-1}_{\leq q})\Big) \to \underline{\mathbb{Z}} \to 0$$

induces a long exact sequence

$$\begin{aligned}\cdots \to H_{r+1}(\mathcal{Q}) \to &\\ &H_r(\mathcal{Q}, q \mapsto \tilde{H}_0(f^{-1}_{\leq q})) \to H_r(\mathcal{Q}, q \mapsto H_0(f^{-1}_{\leq q})) \to H_r(\mathcal{Q}) \to \dots\end{aligned}$$

The lemma follows from the assumption that $\mathcal{Q}$ is contractible. ◻

Corollary 2.7.4. *Let $f : \mathcal{P} \to \mathcal{Q}$ be a poset map such that $\mathcal{Q}$ is contractible and for all $q \in \mathcal{Q}$, $f^{-1}_{\leq q}$ has the homotopy type of a wedge of spheres of dimension 0. Then for $n \geq 0$*

$$\tilde{H}_n(\mathcal{P}) \cong H_n(\mathcal{Q}, q \mapsto \tilde{H}_0(f^{-1}_{\leq q})) \tag{2.39}$$

The left-hand term in Equation (2.39) can be computed using a spectral sequence coming from a filtration of the coefficient functor.

Corollary 2.7.5. *Let $f : \mathcal{P} \to \mathcal{Q}$ be a poset map where $\mathcal{Q}$ is contractible and for all $q \in \mathcal{Q}$, $f^{-1}_{\leq q}$ has the homotopy type of a wedge of spheres of dimension 0. Let d such that $f^{-1}_{\leq q}$ is contractible if $h(q) > d$. There is a spectral sequence*

$$E^1_{rs} = \bigoplus_{\substack{y \in \mathcal{Q} \\ h(y) = d-r}} \tilde{H}_{r+s-1}(\mathcal{Q}_{>y}, \tilde{H}_0(f^{-1}_{\leq y})) \Rightarrow \tilde{H}_{r+s}(\mathcal{P})$$

Proof. Follows from Proposition 2.6.9 applied to the functor $Q \to Ab$ mapping $q \in Q$ to $\tilde{H}_0(f^{-1}_{\leq q})$, and from the previous corollary. ◻

Application to odd order p-groups

Let p be an odd prime. Let P be a p-group with $Z = \Omega_1(Z(P))$ of rank r and suppose that Z is not maximal in $\mathcal{A}_p(P)$. By Lemma 2.3.8 there exists an elementary abelian subgroup E_0 normal in P such that $|E_0 : Z| = p$. Let p^d be the index of $M = C_P(E_0)$ in P. The case $d = 1$ can be dealt with using the Bouc-Thévenaz Wedge Decomposition Formula, so that we are interested here mainly to what happens when $d > 1$.

Let $f : \mathcal{A}_p(P)_{>Z} \to \mathcal{S}_p(P)$ be the poset map defined by $f(A) = AE_0$ and let $\mathcal{E}$ be the poset given by the image of f. In particular, $f(E_0) = E_0 \in \mathcal{E}$ and clearly $f(A) \geq E_0$ for all $A \in \mathcal{A}_p(P)_{>Z}$, so that $\mathcal{E}$ is a cone over E_0.

Our goal is to apply Corollary 2.7.5 and we check first that the assumptions of Corollary 2.7.5 are satisfied.

Lemma 2.7.6. *The poset $\mathcal{E}$ is contractible.*

Recall that if x is an element in a poset $\mathcal{P}$, the height of x in $\mathcal{P}$ is defined as

$$h_{\mathcal{P}}(x) = \max\{h \,|\, x_0 < x_1 < \cdots < x_h \text{ is a chain in } \mathcal{P} \text{ with } x_h \leq x\}.$$

In particular, minimal elements in $\mathcal{P}$ have height 0. When this leads to no confusion, we will omit the subscript and just write $h(x)$ for $h_{\mathcal{P}}(x)$.

Lemma 2.7.7. *Let $R \in \mathcal{E}$, then*

a) R/Z is elementary abelian.

b) R has exponent p.

c) $h_{\mathcal{E}}(R) = \mathrm{rk}(R/Z) - 1$.

Proof. Before proving the assertions, we take a closer look to the action of P on the normal subgroup E_0.

The subgroup E_0 is elementary abelian and can thus be identified with a vector space over $\mathbb{F}_p$. We will often use this fact implicitly from now on. Since E_0 contains Z with index p, i.e. as a subspace of codimension 1, we can choose linearly independent generators $z_1, \ldots, z_r$ and e_0 of E_0 such that $e_0 \in E_0 \backslash Z$ and the elements z_i, $i = 1, \ldots, r$, form a basis of Z.

Let $x \in P$. Since Z is central, we have $xz_ix^{-1} = z_i$, for all $i = 1, \ldots, r$. It follows that P acts on E_0 as linear transformations fixing a hyperplane pointwise. Since P is a p-group this implies that $xe_0x^{-1} = e_0z$ for some $z \in Z$. In other words, the action of any $x \in P$ is represented, relatively to the basis $\{z_1, \ldots, z_r, e_0\}$, by a matrix of the form

$$\left(\begin{array}{ccc|c} & & & * \\ & I_r & & \vdots \\ & & & * \\ \hline 0 & \cdots & 0 & 1 \end{array}\right).$$

It follows in particular that $[x, e_0] \in Z$ for any $x \in P$. We are now in position to prove the assertions.

a) Let $R \in \mathcal{E}$ and let $A \in \mathcal{A}_p(P)_{>Z}$ such that $R = AE_0$. If $A \cap E_0 = E_0$, i.e. $E_0 \leq A$, then $R = A$ is elementary abelian and in particular R/Z is elementary abelian.

Suppose now that $A \cap E_0 \neq E_0$. Since $Z \leq A \cap E_0 \leq E_0$, we have then $A \cap E_0 = Z$. We keep the basis $z_1, \ldots, z_r, e_0$ of E_0 as before and choose linearly independent elements $a_1, \ldots, a_t$ in A such that $\{z_1, \ldots, z_r, a_1, \ldots, a_t\}$ is a basis of A.

The subgroup R is generated by the elements e_0, z_i, a_j for $i = 1, \ldots, r$ and $j = 1, \ldots, t$. From our description of the action of P on E_0, we know that $[a_i, e_0] \in Z$. All other commutators between the chosen generators of R are trivial, so that $[R, R] \leq Z$. As a consequence, R/Z is abelian and since R is generated by elements of order p, R/Z must be elementary abelian and our first assertion is proved.

b) Since R/Z is elementary abelian, we have in particular that R' is central in R. Since R is generated by elements of order p and p is odd, we have that R has exponent p.

c) Let $R_0 < R_1 < \cdots < R_k$ be a chain in $\mathcal{E}$ with $R_k \leq R$. Since R_i belongs to $\mathcal{E}$, we have $Z < E_0 \leq R_i$, for all $i = 0, \ldots, k$. It follows that the chain $R_0/Z < \cdots < R_k/Z$ is a chain of non-trivial subgroups of the elementary abelian group R/Z. Therefore, k is strictly less than the rank of R/Z, i.e. $k \leq \mathrm{rk}(R/Z) - 1$. The height of R in $\mathcal{E}$ is then at most $\mathrm{rk}(R/Z) - 1$, i.e. $h_{\mathcal{E}}(R) \leq \mathrm{rk}(R/Z) - 1$. We prove now the reverse inequality.

Let $A \in \mathcal{A}_p(P)_{>Z}$ such that $R = AE_0$ and let t be the rank of A/Z. Suppose first $E_0 \leq A$, so that $R = A$ is elementary abelian. There exists thus a chain $E_0 = A_0 < A_1 < \cdots < A_{t-1} < A_t = A = R$ of length $\mathrm{rk}(A/Z) - 1 = \mathrm{rk}(R/Z) - 1$. Note that since A is elementary abelian and contains E_0, we have $A_i = A_iE_0 \in \mathcal{E}$ for all $i = 0, \ldots, t$. We have thus a chain of length $\mathrm{rk}(R/Z) - 1$ in $\mathcal{E}_{\leq R}$, i.e. $h_{\mathcal{E}}(R) \geq \mathrm{rk}(R/Z) - 1$.

Suppose now that E_0 is not contained in A, so that $\mathrm{rk}(R/Z) = \mathrm{rk}(A/Z) + 1$. Since A is elementary abelian, we can then choose a chain of subgroups $Z < A_0 < \cdots < A_{t-1} < A_t = A$ of A with $Z < A_0$ and $t = \mathrm{rk}(A/Z)$. For $i = 1, \ldots, t$, let $R_i = A_iE_0$ and let also $R_0 = ZE_0 = E_0$. By definition, $R_i \in E$ for $i = 1, \ldots, t$ and also $R_0 = E_0 \in \mathcal{E}$. Since $R_t = AE_0 = R$, we have thus a chain $R_0 < \cdots < R_t = R$ in $\mathcal{E}$ of length $t = \mathrm{rk}(A/Z) = \mathrm{rk}(R/Z) - 1$. Therefore $h_{\mathcal{E}}(R) \geq \mathrm{rk}(R/Z) - 1$.

$\square$

Lemma 2.7.8. *For $R \in \mathcal{E}$, $f^{-1}_{\leq R} = \mathcal{A}_p(R)_{>Z}$.*

Proof. Let $R \in \mathcal{E}$, we have $f^{-1}_{\leq R} = \{B \in \mathcal{A}_p(P)_{>Z} \,|\, BE_0 \leq R\}$. On the one hand, if $B \in f^{-1}_{\leq R}$, then $Z < B \leq BE_0 \leq R$, so that $B \in \mathcal{A}_p(R)_{>Z}$. On the other hand, if $B \in \mathcal{A}_p(R)_{>Z}$, $B \leq R$, so that $BE_0 \leq RE_0 = R$, hence $B \in f^{-1}_{\leq R}$. $\square$

Let $\mathcal{E}^*$ and $\overline{\mathcal{E}}$ be the subposets of $\mathcal{E}$ defined by

$$\mathcal{E}^* = \{R \in \mathcal{E} \mid R \cap M > E_0\} \cup \{E_0\}$$

and

$$\overline{\mathcal{E}} = \mathcal{E} \backslash \mathcal{E}^* = \{R \in \mathcal{E} \mid E_0 \neq R \text{ and } R \cap M = E_0\}.$$

Remark 2.7.9.

a) We will see that for $R \in \mathcal{E}^*$ the fibers $f^{-1}_{\leq R}$ are contractible, i.e. $f^{-1}_{\leq R} \simeq *$. This is why we have chosen to denote this subposet with a $*$ as a superscript.

b) An element $R \in \overline{\mathcal{E}}$ has not the same height, whether it is considered as an element of $\mathcal{E}$ or $\overline{\mathcal{E}}$. More precisely, $\mathcal{E}_{\leq R} = \overline{\mathcal{E}}_{\leq R} - \{E_0\}$ and since E_0 is minimal in $\mathcal{E}$, we have then $h_{\overline{\mathcal{E}}}(R) = h_{\mathcal{E}}(R) - 1$. In what follows, we will always consider the height of R in $\mathcal{E}$ and we make the convention to write $h(R)$ for $h_{\mathcal{E}}(R)$.

Since $|P : M| = p^d$ we have that $R \cap M > E_0$ if $|R/E_0| \geq p^d$, i.e. if $\mathrm{rk}(R/E_0) \geq d$ or equivalently $\mathrm{rk}(R/Z) > d$. This yields the following lemma, where $h(R)$ is the length of R in $\mathcal{E}$ by convention (see Remark 2.7.9).

Lemma 2.7.10. *For $R \in \overline{\mathcal{E}}$, we have $1 \leq h(R) \leq d$.*

Lemma 2.7.11. *Let $R \in \mathcal{E}$ and let $A \in \mathcal{A}_p(P)_{>Z}$ such that $R = AE_0$. Then,*

a) $A \cap M = Z(R)$.

b) $R \in \overline{\mathcal{E}}$ if and only if $Z(R) = Z$.

Proof.

a) Note that if $E_0 \cap A = E_0$, i.e. $E_0 \leq A$, then $R = A$ is abelian and $A \cap M = A = R = Z(R)$. We suppose now $A \cap E_0 \neq E_0$, i.e. $A \cap E_0 = Z$.

Since $A \cap M$ centralizes E_0 as well as A, we have that $A \cap M$ centralizes $R = AE_0$. Therefore, $A \cap M \leq Z(R)$. Let now $x \in Z(R)$. We must have of course $x \in M$ and it remains to show that x is in A. Since $R = AE_0$, we can write $x = ae$ with $a \in A$ and $e \in E_0$. Since $x \in Z(R)$, we must have $[x, a'] = 1$ for all $a' \in A$. Since $[a, a'] = 1$, we obtain

$$[x, a] = [ae, a'] = [e, a'], \text{ for all } a' \in A.$$

But this implies that e centralizes A and since $e \in E_0$ centralizes E_0, we have $e \in Z$. Therefore $x = ae \in A$, so that $Z(R) \leq A \cap M$.

b) Suppose first $R \in \overline{\mathcal{E}}$, so that $R \neq E_0$ and $R \cap M = E_0$. If $A \cap M = E_0$, i.e. $E_0 \leq A$, then $R = A$. But then $E_0 = A \leq M = A$, so that $R = A = E_0$ which is a contradiction. We must have then $A \cap M \neq E_0$ and in particular $(A \cap M) \cap E_0 = Z$. By assumption $R \cap M = E_0$, so that $A \cap M \leq R \cap M = E_0$ and it follows that $A \cap M = Z$. By part a), this is equivalent to $Z(R) = Z$.

Suppose now $Z(R) = Z$. It follows from part a) that $A \cap M = Z$. But A has index p in R, so that $A \cap M$ has index p in $R \cap M$. Since $E_0 \leq R \cap M$, this implies $R \cap M = E_0$.

□

Lemma 2.7.12. *Let $R \in \overline{\mathcal{E}}$ with $h(R) \geq 2$ and let $B \in \mathcal{A}_p(P)_{>Z}$ such that $R = BE_0$. Then*

a) For any $A \in \mathcal{A}_p(R)_{>Z}$, we have $A \leq B$ if $\mathrm{rk}(A/Z) \geq 2$.

b) B is the unique subgroup in $\mathcal{A}_p(P)_{>Z}$ such that $R = BE_0$.

c) The poset $\mathcal{A}_p(R)_{>Z}$ is the disjoint union of $\mathcal{A}_p(B)_{>Z}$ and $p^{h(R)}$ isolated vertices, corresponding to the subgroups $A \in \mathcal{A}_p(R)_{>Z}$ with $\mathrm{rk}(A/Z) = 1$ *that are not contained in B.*

Proof. We begin with some deductions on the structure of R and introduce some notation. Since $R \in \overline{\mathcal{E}}$, we have $B \cap M = Z$ by Lemma 2.7.11. We have in particular $R \neq B$, so that $|R : B| = p$. This, together with Lemma 2.7.7, implies that $\mathrm{rk}(B/Z) = \mathrm{rk}(R/Z) - 1 = h(R) \geq 2$.

Let $b_1, \dots, b_t$ be elements of B such that the left cosets $b_i Z$, $i = 1, \dots, t$ form a basis of B/Z. In other words, $\{b_1, \dots, b_t\}$ is a basis of a complement to Z in B. Let $e_0 \in E_0 \backslash Z$. Since R/Z is elementary abelian (see Lemma 2.7.7), there exists $z_i \in Z$ such that $b_i e_0 b_i^{-1} = z_i e_0$, for any $i = 1, \dots, t$.

The next step is to show that these elements $z_1, \dots, z_t \in Z$ are linearly independent. Suppose thus that $\prod_{i=1}^t z_i^{a_i} = 1$. Let b be the element defined by

$$b = \prod_{i=1}^{t} b_i^{a_i}.$$

Note that since B acts trivially on Z, we have $b_i^k e_0 b_i^{-k} = z_i^k e_0$, for any $k \in \mathbb{Z}$. It follows that

$$be_0 b^{-1} = \left(\prod_{i=1}^{t} z_i^{a_i} \right) e_0 = e_0.$$

We have thus $b \in B \cap M = Z$, hence $b \in Z$. Since the left cosets $\{b_i Z\}$ form a basis of B/Z, it follows that $b_i^{a_i} \in Z$ and hence $a_i \equiv 0 \mod p$ for all $i = 1, \dots, t$. Therefore, $z_i^{a_i} = 1$ for all $i = 1, \dots, t$, showing that the elements $z_1, \dots, z_t$ are linearly independent.

a) Let $A \in \mathcal{A}_p(R)_{>Z}$ with $\mathrm{rk}(A/Z) \geq 2$, we prove that $A \leq B$. Since $\mathrm{rk}(A/Z)$ is at least 2, we can choose $x, y \in A$ such that the left cosets xZ and yZ are linearly independent in A/Z. Note that in particular, $x, y \notin Z$.

   The subgroup E_0 is generated by Z and the element $e_0 \in E_0 \backslash Z$. The subgroup B is generated by Z and the linearly independent elements $b_1, \dots, b_t$. It follows that R is generated by Z, e_0 and $b_1, \dots, b_t$. We can then write x, y as products of these generators:

$$x = ze_0^{\gamma} \prod_{i=1}^{t} b_i^{x_i} \quad \text{and} \quad y = we_0^{\delta} \prod_{i=1}^{t} b_i^{y_i}, \quad \text{with } z, w \in Z.$$

Since R/Z is elementary abelian, we have in particular $[R,R] \leq Z$, so that commutators can be calculated easily in R. We have

$$[x,y] = \prod_{i=1}^{t} \left([e_0^{\gamma}, b_i^{y_i}] \cdot [b_i^{x_i}, e_0^{\delta}]\right) = \prod_{i=1}^{t} z_i^{\delta x_i - \gamma y_i}.$$

Since the elements z_i, $i = 1, \ldots, t$, are linearly independent, we have then

$$[x,y] = 1 \iff \delta x_i - \gamma y_i \equiv 0 \mod p, \text{ for all } i = 1, \ldots, t. \tag{2.40}$$

If $\gamma \not\equiv 0 \mod p$ and $\delta \equiv 0 \mod p$, then $e_0^{\delta} \in Z$ and (2.40) yields $-\gamma y_i \equiv 0 \mod p$ for all $i = 1, \ldots, t$. Since γ is invertible modulo p, we have thus $y_i \equiv 0 \mod p$, for all $i = 1, \ldots, t$. Therefore, $b_i^{y_i} \in Z$ for all $i = 1, \ldots, t$, showing that $y \in Z$, which is a contradiction.

If $\gamma \equiv 0 \mod p$ and $\delta \not\equiv 0 \mod p$, we obtain similarly $x \in Z$, which is also a contradiction.

Suppose now $\gamma \not\equiv 0 \mod p$ and $\delta \not\equiv 0 \mod p$. We have then $x_i \equiv (\gamma\delta^{-1})y_i \mod p$ and therefore

$$x = ze_0^{\gamma} \prod_{i=1}^{t} b_i^{x_i} = ze_0^{\gamma} \prod_{i=1}^{t} b_i^{(\gamma\delta^{-1})y_i} = z' \left(e_0^{\delta} \prod_{i=1}^{t} b_i^{y_i}\right)^{\gamma\delta^{-1}} = z'' y^{\gamma\delta^{-1}}.$$

But this contradicts the linear independence of xZ and yZ.

We are thus left with the case $\gamma \equiv \delta \equiv 0 \mod p$. But in this situation, $e_0^{\gamma}, e_0^{\delta} \in Z$, so that $x, y \in B$.

Since this is true for any pair x, y with xZ and yZ linearly independent, this shows that $A \leq B$.

b) By part a), the subgroup B contains all subgroups $A \in \mathcal{A}_p(R)_{>Z}$ with $\mathrm{rk}(A/Z) \geq 2$. It follows that B is maximal among those subgroups and hence is unique.

c) Part a) implies immediately that $\mathcal{A}_p(P)_{>Z}$ consists of isolated vertices and one contractible component, namely $\mathcal{A}_p(B)_{>Z}$. Recall from Lemma 2.7.7 that R has exponent p, hence any subgroup A of R with $|A : Z| = p$ is elementary abelian. It follows that the number of isolated vertices is equal to the number of complements to the hyperplane B/Z in R/Z. This is a standard calculation and we obtain thus $p^{\mathrm{rk}(R/Z)-1} = p^{h(R)}$.

□

We are now in position to describe the fibers of $f : \mathcal{A}_p(P)_{>Z} \to \mathcal{E}$.

Lemma 2.7.13. *Let $R \in \mathcal{E}$, then*

a) if $R \in \mathcal{E}^*$, $f^{-1}_{\leq R} = \mathcal{A}_p(R)_{>Z}$ is contractible;

b) if $R \in \overline{\mathcal{E}}$, $f^{-1}_{\leq R} = \mathcal{A}_p(R)_{>Z}$ has the homotopy type of a wedge of $p^{h(R)}$ spheres of dimension 0.

Proof. Recall first from Lemma 2.7.8 that $f^{-1}_{\leq R} = \mathcal{A}_p(R)_{>Z}$.

a) Suppose $R \in \mathcal{E}^*$. If $R = E_0$, $\mathcal{A}_p(R)_{>Z} = \{E_0\}$ is a point. Suppose now $R \neq E_0$ and let $B \in \mathcal{A}_p(P)_{>Z}$ such that $R = BE_0$. By Lemma 2.7.11, we have $Z(R) > Z$. We have thus that $Z(R)$ is a conjunctive element in $\mathcal{A}_p(R)_{>Z}$, which is then contractible.

b) Suppose now $R \in \overline{\mathcal{E}}$. When $h(R) \geq 2$, the result follows from Lemma 2.7.12. When $h(R) = 1$, $|R/Z| = p^2$, so that $\mathcal{A}_p(R)_{>Z}$ is isomorphic to the poset of proper subspaces in R/Z, hence consists of $p+1$ points.

□

We can now apply Corollary 2.7.5 to the map $f : \mathcal{A}_p(P) \to \mathcal{E}$ and we obtain the following result.

Proposition 2.7.14. *Let p be an odd prime and let P be a p-group such that $Z = \Omega_1(Z(P))$ is not maximal in $\mathcal{A}_p(P)$. Let E_0 be a normal minimal element in $\mathcal{A}_p(P)_{>Z}$ and let p^d be the index of $C_P(E_0)$ in P. Let $\mathcal{E}$ be the image of the poset map $f : \mathcal{A}_p(P)_{>Z} \to \mathcal{S}_p(P)$ defined by $f(A) = AE_0$ and let also $\overline{\mathcal{E}} = \{R \in \mathcal{E} \mid R \neq E_0 \text{ and } R \cap M = E_0\}$.*

There is a spectral sequence E^1_{rs} converging to $\tilde{H}_{r+s}(\mathcal{A}_p(P)_{>Z})$, with $E^1_{rs} = 0$ if $r \geq d$ and

$$E^1_{rs} = \bigoplus_{\substack{R \in \overline{\mathcal{E}} \\ h(R) = d-r}} \tilde{H}_{r+s-1}\left(\mathcal{E}_{>R}, \mathbb{Z}^{p^{d-r}}\right), \text{ if } 0 \leq r \leq d-1.$$

Proof. We have seen in Lemma 2.7.6 that the poset $\mathcal{E}$ is contractible. Furthermore, Lemma 2.7.13 implies that $f^{-1}_{\leq R}$ has the homotopy type of a wedge of spheres of dimension 0 if $R \in \overline{\mathcal{E}}$, and is contractible otherwise. This, together with Lemma 2.7.7, shows in particular that $f^{-1}_{\leq R}$ is contractible if $h(R) > d$. All the assumptions of Corollary 2.7.5 are thus satisfied, so that we obtain a spectral sequence E^1_{rs} converging to $\tilde{H}(\mathcal{A}_p(P)_{>Z})$, with $E^1_{rs} = 0$ for $r > d$ and

$$E^1_{rs} = \bigoplus_{\substack{R \in \mathcal{E} \\ h(R) = d-r}} \tilde{H}_{r+s-1}\left(\mathcal{E}_{>R}, \tilde{H}_0(f^{-1}_{\leq R})\right), \text{ if } r \leq d.$$

If $R \notin \overline{\mathcal{E}}$, then $f^{-1}_{\leq R}$ is contractible and hence $\tilde{H}_0(f^{-1}_{\leq R}) = 0$. We have thus

$$E^1_{rs} = \bigoplus_{\substack{R \in \overline{\mathcal{E}} \\ h(R) = d-r}} \tilde{H}_{r+s-1}\left(\mathcal{E}_{>R}, \tilde{H}_0(f^{-1}_{\leq R})\right), \text{ if } r \leq d.$$

Since $h(R) \geq 1$ for $R \in \overline{\mathcal{E}}$, we have in particular $\tilde{H}_0(f^{-1}_{\leq R}) = 0$ for any $R \in \mathcal{E}$ with $h(R) = 0$, i.e. if $R = E_0$. It follows that $E^1_{rs} = 0$ if $r = d$, so that now $E^1_{rs} = 0$ for $r \geq d$.

We remark finally that if $R \in \overline{\mathcal{E}}$, then $\tilde{H}_0(f^{-1}_{\leq R}) = \tilde{H}_0(\mathcal{A}_p(R)_{>Z})$ is isomorphic with $\mathbb{Z}^{p^{h(R)}}$, thanks to corollary 2.7.13 and the proposition is proved. □

In order to use this spectral sequence, we need to understand the upper intervals $\mathcal{E}_{>R}$ for $R \in \overline{\mathcal{E}}$. When $h(R) \geq 2$, we have the following result expressing $\mathcal{E}_{>R}$ in terms of upper intervals in $\mathcal{A}_p(P)$.

Lemma 2.7.15. *If $R = BE_0 \in \overline{\mathcal{E}}$ with $h(R) \geq 2$, then $\mathcal{E}_{>R} \simeq \mathcal{A}_p(P)_{>B}$.*

Proof. Consider the poset map $g : \mathcal{A}_p(P)_{>B} \to \mathcal{E}_{>R}$ given by $g(B') = B'E_0$ and let $S \in \mathcal{E}_{>R}$. By the Quillen fiber lemma, we only have to show that $g^{-1}_{\leq S}$ is contractible. It is immediate that $g^{-1}_{\leq S} = \mathcal{A}_p(S)_{>B}$.

If $S \in \overline{\mathcal{E}}$, then $S = B'E_0$ for a unique $B' \in \mathcal{A}_p(P)_{>Z}$. Since $h(R) \geq 2$, we have $\mathrm{rk}(B/Z) \geq 2$ and thus $B \leq B'$ by Lemma 2.7.12. We have thus $\mathcal{A}_p(S)_{>B} = \mathcal{A}_p(B')_{>B}$ which is a cone on B' hence is contractible.

Suppose now $S \in \mathcal{E}^*$. Remark first that $S \not\leq M$, since $R \not\leq M$. In particular, $S \neq E_0$. We can choose $B' \in \mathcal{A}_p(P)_{>Z}$ such that $S = B'E_0$. And now $Z(S) = B' \cap M > Z$ by Lemma 2.7.11.

If $Z(S) \leq B$, then there exists $b \in B \backslash Z$ with $b \in Z(S)$. In particular, b centralizes E_0, but this is a contradiction since we have $B \cap M = Z$ by Lemma 2.7.11. We have thus that $BZ(S)$ strictly contains B and hence $BZ(S) \in \mathcal{A}_p(S)_{>B}$. For any $A \in \mathcal{A}_p(S)_{>B}$, we also have $AZ(S) \in \mathcal{A}_p(S)_{>B}$ and the following inequalities show that the poset $\mathcal{A}_p(S)_{>B}$ is (conically) contractible:

$$A \leq AZ(S) \geq BZ(S), \text{ for any } A \in \mathcal{A}_p(S)_{>B}.$$

In all cases, we have that $g^{-1}_{\leq S} = \mathcal{A}_p(S)_{>B}$ is contractible and the lemma is proved. □

Unfortunately, we don't have a good description of $\mathcal{E}_{>R}$ in general when $h(R) = 1$. We shall now give two situations in which the poset $\mathcal{E}_{>R}$ can be described more precisely.

Lemma 2.7.16. *Let $R \in \overline{\mathcal{E}}$ with $h(R) = 1$ and let $A \in \mathcal{A}_p(P)_{>Z}$ such that $R = AE_0$. Suppose that $B \cap M$ strictly contains Z for all $B \in \mathcal{A}_p(P)_{>Z}$ with $\mathrm{rk}(B/Z) \geq 2$ and $BE_0 > R$. Then*

$$\mathcal{E}_{>R} \simeq \mathcal{A}_p(P)_{>A}.$$

Proof. Let $g : \mathcal{A}_p(P)_{>A} \to \mathcal{E}_{>R}$ be the poset map defined by $g(B') = B'E_0$. By the Quillen fiber lemma, it is enough to show that the fibers $g^{-1}_{\leq S}$ are contractible for any $S \in \mathcal{E}_{>R}$. It is immediate that $g^{-1}_{\leq S} = \mathcal{A}_p(S)_{>A}$.

Let $B' \in \mathcal{A}_p(P)_{>Z}$ such that $S = B'E_0$. Since $h(S) > h(R) = 1$, we have $\mathrm{rk}(B'/Z) \geq 2$ and hence $Z(S) = B' \cap M > Z$. The poset $\mathcal{A}_p(S)_{>A}$ is now (conically) contractible via the following inequalities:

$$E \leq EZ(S) \geq AZ(S), \text{ for any } E \in \mathcal{A}_p(S)_{>A}.$$

□

Remark 2.7.17. The assumption made in the statement of the previous lemma is equivalent to require that $Z(S)$ strictly contains Z for all $S \in \mathcal{E}_{>R}$. This implies in particular that $\overline{\mathcal{E}} = \{R_1, \dots, R_k\}$, with $h(R_i) = 1$ for $i = 1, \dots, k$, so that $\overline{\mathcal{E}}$ consists of isolated vertices.

Recall that d is defined as the p-valuation of the index of $M = C_P(E_0)$ in P. The situation of Lemma 2.7.16 happens in the particular case $d = 1$, i.e. $|P : M| = p$. Indeed, if $B \in \mathcal{A}_p(P)_{>Z}$ is such that $\mathrm{rk}(B/Z) \geq 2$, then on the one hand $|B : Z| \geq p^2$. Since $|P : M| = p$, we have on the other hand that $B \cap M$ has index p in B, so that $B \cap M > Z$. The last assertion of the following proposition shows that, in this situation, the spectral sequence derived in Proposition 2.7.14 yields exactly the same result that what we would have obtained by simply applying the homological version of the Bouc-Thévenaz Wedge Decomposition Formula.

Proposition 2.7.18. *Let p be an odd prime and let P be a p-group such that $Z = \Omega_1(Z(P))$ is not maximal in $\mathcal{A}_p(P)$. Let E_0 be a normal minimal element in $\mathcal{A}_p(P)_{>Z}$ and let p^d be the index of $C_P(E_0)$ in P. Let $\mathcal{E}$ be the image of the poset map $f : \mathcal{A}_p(P)_{>Z} \to \mathcal{S}_p(P)$ defined by $f(A) = AE_0$ and let also $\overline{\mathcal{E}} = \{R \in \mathcal{E} \,|\, R \neq E_0 \text{ and } R \cap M = E_0\}$.*

Assume that $B \cap M$ strictly contains Z, for any $B \in \mathcal{A}_p(P)_{>Z}$ such that $\mathrm{rk}(B/Z) \geq 2$. Then

a) For all $R \in \overline{\mathcal{E}}$ with $h(R) = 1$, we have $\mathcal{E}_{>R} \simeq \mathcal{A}_p(P)_{>A}$, where A is chosen arbitrarily such that $R = AE_0$.

b) There is a spectral sequence E^1_{rs} converging to $\tilde{H}_{r+s}(\mathcal{A}_p(P)_{>Z})$, with $E^1_{rs} = 0$ if $r \neq d-1$ and

$$E^1_{d-1,s} = \bigoplus_{\substack{R \in \overline{\mathcal{E}} \\ h(R)=1}} \tilde{H}_{d+s-2}(\mathcal{E}_{>R}, \mathbb{Z}^p).$$

c) For all $n \geq 0$, we have

$$\tilde{H}_n(\mathcal{A}_p(P)_{>Z}) \cong \bigoplus_{\substack{R \in \overline{\mathcal{E}} \\ h(R)=1}} \tilde{H}_{n-1}(\mathcal{E}_{>R}, \mathbb{Z}^p).$$

d) For all $n \geq 0$, we have

$$\tilde{H}_n(\mathcal{A}_p(P)_{>Z}) \cong \bigoplus_{F \in \mathcal{F}} \tilde{H}_{n-1}(\mathcal{A}_p(C_M(F))_{>Z}),$$

where $\mathcal{F} = \{F \in \mathcal{A}_p(P)_{>Z} \,|\, F \cap M = Z\}$.

Proof.

a) Follows immediately from Lemma 2.7.16.

b) Recall from Proposition 2.7.14 that there is a spectral sequence E^1_{rs} converging to $\tilde{H}_{r+s}(\mathcal{A}_p(P)_{>Z})$, with $E^1_{rs} = 0$ for $r \geq d$ and

$$E^1_{rs} = \bigoplus_{\substack{R \in \overline{\mathcal{E}} \\ h(R)=d-r}} \tilde{H}_{r+s-1}(\mathcal{E}_{>R}, \mathbb{Z}^{p^{d-r}}), \text{ if } 0 \leq r \leq d-1.$$

It remains to show that $E^1_{rs} = 0$ for $r \leq d-2$. Let $R \in \overline{\mathcal{E}}$ and let $A \in \mathcal{A}_p(P)_{>Z}$ such that $R = AE_0$. If $h(R) \geq 2$, then $\mathrm{rk}(A/Z) \geq 2$ and thus $A \cap M > Z$ which is in contradiction with Lemma 2.7.11. It follows that R must have height 1 and thus $E^1_{rs} = 0$ for $r \leq d-2$.

c) The spectral sequence obtained in b) has all its non-zero terms concentrated in the $(d-1)$-th column. It follows that $E^1_{rs} = E^\infty_{rs}$ and hence

$$\tilde{H}_n(\mathcal{A}_p(P)_{>Z}) \cong E^1_{d-1,n-d+1} = \bigoplus_{\substack{R\in\overline{\mathcal{E}} \\ h(R)=1}} \tilde{H}_{n-1}(\mathcal{E}_{>R}, \mathbb{Z}^p).$$

d) Let $R \in \overline{\mathcal{E}}$. Since $B \cap M > Z$ for all $B \in \mathcal{A}_p(P)_{>Z}$ such that $\mathrm{rk}(B/Z) \geq 2$, we must have $h(R) = 1$. Since R/Z is elementary abelian of rank 2 and R has exponent p, we have that $\mathcal{A}_p(R)_{>Z}$ consists of $p+1$ isolated points. More precisely,

$$\mathcal{A}_p(R)_{>Z} = \{E_0, A_1, \ldots, A_p\}.$$

By Lemma 2.7.16, we have also that $\mathcal{E}_{>R}$ is homotopy equivalent to $\mathcal{A}_p(P)_{>A}$ for any A such that $R = AE_0$. It follows that $\mathcal{E}_{>R}$ is homotopy equivalent to $\mathcal{A}_p(P)_{>A_i}$ for any $i = 1, \ldots, p$. In particular, $\mathcal{A}_p(P)_{>A_i}$ is homotopy equivalent to $\mathcal{A}_p(P)_{>A_j}$ for any $1 \leq i, j \leq p$. Putting everything together, we have now

$$\tilde{H}_{n-1}(\mathcal{E}_{>R}, \mathbb{Z}^p) \cong \bigoplus_{i=1}^{p} \tilde{H}_{n-1}(\mathcal{E}_{>R}) \cong \bigoplus_{i=1}^{p} \tilde{H}_{n-1}(\mathcal{A}_p(P)_{>A_i})$$

To finish the proof, it is now enough to remark that

$$\mathcal{F} = \coprod_{R\in\overline{\mathcal{E}}} \mathcal{A}_p(R)_{>Z} \setminus \{E_0\},$$

and that $\mathcal{A}_p(P)_{>A_i}$ is homotopy equivalent to $\mathcal{A}_p(C_M(A_i))_{>Z}$. This last equivalence comes from the fact that, for any $B \in \mathcal{A}_p(P)_{>A_i}$, we have $\mathrm{rk}(B) \geq 3$, hence $B \cap M > Z$ by assumption. We can thus define a poset map $f : \mathcal{A}_p(P)_{>A_i} \to \mathcal{A}_p(C_M(A_i))_{>Z}$ by $f(B) = B \cap M$. This map has a homotopy inverse given by the poset map $g : \mathcal{A}_p(C_M(A_i))_{>Z} \to \mathcal{A}_p(P)_{>A_i}$ given by $g(E) = EA_i$.

□

We turn now our attention to another special case in which $\mathcal{E}_{>R}$ can be described for $R \in \overline{\mathcal{E}}$ with $h(R) = 1$.

Lemma 2.7.19. *Let $R \in \overline{\mathcal{E}}$ with $h(R) = 1$. If $C_P(R) = Z$, then*

$$\mathcal{E}_{>R} \cong \coprod_{\substack{A\in\mathcal{A}_p(R)_{>Z} \\ A\neq E_0}} \mathcal{A}_p(P)_{>A}$$

Proof. Since R/Z is elementary abelian of rank 2 and R has exponent p, we have that $\mathcal{A}_p(R)_{>Z}$ consists of $p+1$ isolated points and more precisely

$$\mathcal{A}_p(R)_{>Z} = \{E_0, A_1, \ldots, A_p\}.$$

Remark that since R is not abelian, we have $\mathcal{A}_p(P)_{>A_i} \cap \mathcal{A}_p(P)_{>A_j} = \emptyset$, for $1 \leq i \neq j \leq p$. Let us write $\mathcal{A}$ for the disjoint union $\coprod_{i=1}^p \mathcal{A}_p(P)_{>A_i}$. There is a natural poset map $g : \mathcal{A} \to \mathcal{E}_{>R}$ sending $E \in \mathcal{A}_p(P)_{>A_i}$ to EE_0.

Let $S \in \mathcal{E}_{>R}$ and let $B \in \mathcal{A}_p(P)_{>Z}$ be such that $S = BE_0$. We have that $B \cap M$ centralizes E_0 and B, hence centralizes S and thus also R. Since $C_P(R) = C_M(R) = Z$, we must have $B \cap M = Z$. It follows then by Lemma 2.7.11 that $S \in \overline{\mathcal{E}}$ and therefore B is unique with the property $S = BE_0$, by Lemma 2.7.12.

Since $|S : B| = p$ and $E_0 \leq R$, we have also $|R : B \cap R| = p$. In particular, $B \cap R > Z$, so that there exists $1 \leq j \leq p$ such that $A_j = \cap R$. Furthermore, this A_j is uniquely determined since the posets $\mathcal{A}_p(P)_{>A_i}$ are disjoint.

We denote by $q : \mathcal{E}_{>R} \to \mathcal{A}$ the poset map sending $S \in \mathcal{E}_{>R}$ to B in the component $\mathcal{A}_p(P)_{>A_j}$, where B is the unique elementary abelian subgroup of P such that $S = BE_0$ and j is the only index is such that $A_j = B \cap R$.

We show now that g and q are mutually inverse. If $B > A_i$ for some i, then $A_i \leq BE_0$, so that $qg(B) = B$. In the other direction, for $S = BE_0 \in \mathcal{E}_{>R}$, we have $gq(S) = g(B) = BE_0 = S$. It follows that gq and qg are the identity, so that $\mathcal{E}_{>R}$ is thus isomorphic to $\mathcal{A}$. □

The situation of Lemma 2.7.19, that is $C_P(R) = Z$ for all $R \in \overline{\mathcal{E}}$ with $h(R) = 1$, can happen only if the poset $\mathcal{F} = \{F \in \mathcal{A}_p(P)_{>Z} \,|\, F \cap M = Z\}$ and the poset $\mathcal{A}_p(M)_{>Z}$ are disjoint. In particular, the poset $\mathcal{A}_p(P)_{>Z}$ is the disjoint union of the contractible component $\mathcal{A}_p(M)_{>Z}$ and of the poset $\mathcal{F}$. Except for what concerns the connected components, the homotopy type of $\mathcal{A}_p(P)_{>Z}$ is thus determined by $\mathcal{F}$.

In the situation of Lemma 2.7.19, that is $C_P(R) = Z$ for all $R \in \overline{\mathcal{E}}$ with $h(R) = 1$, the spectral sequence derived in Proposition 2.7.14 does not converge immediately. The best we can say is the content of the following proposition. Note that this is consistent with our previous discussion, since the following result shows that the homology groups of $\mathcal{A}_p(P)_{>Z}$ are determined by the poset $\mathcal{F}$.

Proposition 2.7.20. *Let p be an odd prime and let P be a p-group such that $Z = \Omega_1(Z(P))$ is not maximal in $\mathcal{A}_p(P)$. Let E_0 be a normal minimal element in $\mathcal{A}_p(P)_{>Z}$ and let p^d be the index of $C_P(E_0)$ in P. Let $\mathcal{E}$ be the image of the poset map $f : \mathcal{A}_p(P)_{>Z} \to \mathcal{S}_p(P)$ defined by $f(A) = AE_0$ and let also $\overline{\mathcal{E}} = \{R \in \mathcal{E} \,|\, R \neq E_0$ and $R \cap M = E_0\}$*

Assume that $C_P(R) = Z$ for all $R \in \overline{\mathcal{E}}$ with $h(R) = 1$. There is a spectral sequence E^1_{rs} converging to $\tilde{H}_{r+s}(\mathcal{A}_p(P)_{>Z})$, with $E^1_{rs} = 0$ if $r \geq d$ and

$$E^1_{rs} = \bigoplus_{F \in \mathcal{F}} \tilde{H}_{d+s-2}\left(\mathcal{A}_p(P)_{>F}, \mathbb{Z}^{\mathrm{rk}(F/Z)}\right), \ \text{if } 0 \leq r \leq d-1,$$

where $\mathcal{F} = \{F \in \mathcal{A}_p(P)_{>Z} \,|\, F \cap M = Z\}$.

Proof. Recall from Proposition 2.7.14 that there is a spectral sequence E^1_{rs} converging to $\tilde{H}_{r+s}(\mathcal{A}_p(P)_{>Z})$, with $E^1_{rs} = 0$ for $r \geq d$ and

$$E^1_{rs} = \bigoplus_{\substack{R \in \overline{\mathcal{E}} \\ h(R) = d-r}} \tilde{H}_{r+s-1}(\mathcal{E}_{>R}, \mathbb{Z}^{p^{d-r}}), \ \text{if } 0 \leq r \leq d-1.$$

Since $C_P(R) = Z$, the poset $\mathcal{F}$ is the union of $\left\{R \in \overline{\mathcal{E}} \,|\, h(R) \geq 2\right\}$ and of the posets $\mathcal{A}_p(R)_{>Z} \setminus \{E_0\}$, where R ranges over all $R \in \overline{\mathcal{E}}$ with $h(R) = 1$.

Let $R \in \overline{\mathcal{E}}$ with $h(R) = 1$. It follows from Lemma 2.7.19 that $\tilde{H}_n(\mathcal{E}_{>R})$ is isomorphic to the direct sum

$$\bigoplus_{A \in \mathcal{A}_p(R)_{>Z} \setminus \{E_0\}} \tilde{H}_n(\mathcal{A}_p(P)_{>A}).$$

The proposition follows now from the observation that since $C_P(R) = Z$, the poset $\mathcal{F}$ is the union of $\{R \in \overline{\mathcal{E}} \mid h(R) \geq 2\}$ and of the posets $\mathcal{A}_p(R)_{>Z} \setminus \{E_0\}$, where R ranges over all $R \in \overline{\mathcal{E}}$ with $h(R) = 1$. $\square$

In general, we don't have a good description of the poset $\mathcal{E}_{>R}$, for $R \in \overline{\mathcal{E}}$ with $h(R) = 1$. A good description would be to have an expression of $\mathcal{E}_{>R}$ in term of upper intervals of the form $\mathcal{A}_p(P)_{>A}$ with $A \in \mathcal{A}_p(R)_{>Z} \setminus \{E_0\}$. Note that this was the case in the two previous special situations. The best we can do towards such a description of $\mathcal{E}_{>R}$ is the following.

Let $R \in \overline{\mathcal{E}}$ with $h(R) = 1$ and let $\mathcal{A}_R$ be the poset defined as the disjoint union

$$\mathcal{A}_R = \coprod_{A \in \mathcal{A}_p(R)_{>Z} A \neq E_0} \mathcal{A}_p(P)_{>A}.$$

We can define a relation $\sim$ on the poset $\mathcal{A}_R$ in the following manner. Let $A_1, A_2 \in \mathcal{A}_p(R)_{>Z} \setminus \{E_0\}$ and let $B_1, B_2 \in \mathcal{A}_R$ with $A_1 < B_1$ and $A_2 < B_2$.

If $A_1 = A_2$, then $B_1 \sim B_2$ if and only if $B_1 = B_2$. If $A_1 \neq A_2$, then $B_1 \sim B_2$ if and only if $|B_i : B_i \cap M| = p$ for $i = 1, 2$ and $B_1 \cap M = B_2 \cap M \in \mathcal{A}_p(M)_{>Z}$.

Let us explain briefly the meaning of this condition. Suppose $B_1 \sim B_2$ with $A_1 \neq A_2$ and let $C = B_1 \cap M = B_2 \cap M$. Remark first that C centralizes R, so that in fact $C \in \mathcal{A}_p(C_M(R)_{>Z}) = \mathcal{A}_p(C_P(R)_{>Z})$. The condition that $|B_i : B_i \cap M| = p$, for $i = 1, 2$, implies that C is maximal in B_1 and in B_2 and thus $B_i = CA_i$ for $i = 1, 2$. We see then that the relation $\sim$ identifies CA_1 with CA_2 for any $A_1, A_2 \in \mathcal{A}_p(R)_{>Z} \setminus \{E_0\}$ and any $C \in \mathcal{A}_p(C_P(R)_{>Z})$.

It is not difficult to check that $\sim$ is an equivalence relation on $\mathcal{A}_R$ and we define $\mathcal{D}_R$ as the quotient

$$\mathcal{D}_R = \mathcal{A}_R / \sim .$$

For $B \in \mathcal{A}_R$ we denote by $[B]$ the class of B in $\mathcal{D}_R$. For B_1 and B_2 in $\mathcal{A}_r$, we define $[B_1] \leq [B_2]$ if and only if there exists $B_1' \sim B_1$ and $B_2' \sim B_2$ with $B_1' \leq B_2'$. Now $\mathcal{D}_R$ is a poset with respect to this partial order $\leq$.

Lemma 2.7.21. *Let $R \in \overline{\mathcal{E}}$ with $h(R) = 1$. There is a homotopy equivalence*

$$\mathcal{E}_{>R} \simeq \mathcal{D}_R.$$

Proof. There is a natural map $\mathcal{A}_R \to \mathcal{E}_{>R}$ sending B to BE_0. Suppose $B_1 \sim B_2$, then $B_1 = CA_1$ and $B_2 = CA_2$ for some $C \in \mathcal{A}_p(C_P(R)_{>Z})$. Since $R = A_1E_0 = A_2E_0$, we have $B_1E_0 = CA_1E_0 = CR = CA_2E_0 = B_2E_0$. There is thus an induced map $g : \mathcal{D}_R \to \mathcal{E}_{>R}$.

In the other direction, we define a map $q : \mathcal{E}_{>R} \to \mathcal{D}_R$ in the following way. Let $S \in \mathcal{E}_{>R}$ and let B such that $R = BE_0$.

If $R \in \overline{\mathcal{E}}$, then B is unique such that $R = BE_0$ and $B \cap R$ contains a unique A_j in $\mathcal{A}_p(R)_{>Z} \setminus \{E_0\}$. In this situation, we send S to $[B] \in \mathcal{D}_R$.

If $R \notin \overline{E}$, then $B \cap M > Z$ and we send S to $[(B \cap M)A]$, where A can be any subgroup in $\mathcal{A}_p(R)_{>Z} \setminus \{E_0\}$. This is independent of the choice of A because of the definition of $\sim$.

It is not difficult to check that $gq \leq \mathrm{id}$ and $qg \leq \mathrm{id}$, showing that $\mathcal{E}_{>R}$ is homotopy equivalent to $\mathcal{D}_R$. $\square$

Remark 2.7.22. The two special cases treated previously correspond to the two extreme cases. If $B \cap M > Z$ for any $B \in \mathcal{A}_p(P)_{>Z}$ with $\mathrm{rk}(R/Z) \geq 2$, then all subgroups in $\mathcal{A}_R$ are equivalent with respect to $\sim$. In this situation, we see that $\mathcal{E}_{>R} \simeq \mathcal{D}_R \cong \mathcal{A}_p(P)_{>A}$ for an arbitrary chosen $A \in \mathcal{A}_p(R)_{>Z} \setminus \{E_0\}$. If $C_P(R) = Z$, then no subgroups are identified by $\sim$, so that $\mathcal{E}_{>R} \simeq \mathcal{D}_R = \mathcal{A}_R$. In both cases, we recover the previous results.

Note that the presence of these two extreme cases seems to suggest that there is no easy description of $\mathcal{E}_{>R}$ in the intermediate cases.

2.8 Fiber theorems

Useful tools in topology of posets are the so-called "fiber theorems". They have the following general form: given a poset map $f : \mathcal{P} \to \mathcal{Q}$, certain properties can be transferred from $\mathcal{P}$ to $\mathcal{Q}$ if the fibers $f^{-1}(\mathcal{Q}_{\leq q})$ are sufficiently well-behaved. Maybe the best known of this family of results is the so-called "Quillen fiber lemma" asserting that $\mathcal{P}$ and $\mathcal{Q}$ are homotopy equivalent if the fibers are contractible.

A general result subsuming several known fiber theorems, including the Quillen fiber lemma, was proved by Björner, Wachs and Welker.

Theorem 2.8.1 (Björner, Wachs, Welker)**.** *Let $f : \mathcal{P} \to \mathcal{Q}$ be a poset map such that for all $q \in \mathcal{Q}$ the fiber $f^{-1}_{\leq q}$ is non-empty, and for all non-minimal $q \in \mathcal{Q}$ there exists $c_q \in f^{-1}_{\leq q}$ such that the inclusion map $f^{-1}_{<q} \hookrightarrow f^{-1}_{\leq q}$ is homotopic to the constant map sending $f^{-1}_{<q}$ to c_q. Then P is homotopy equivalent to the wedge*

$$\mathcal{Q} \vee \bigvee_{q \in \mathcal{Q}} \left(f^{-1}_{\leq q} * \mathcal{Q}_{>q} \right)$$

For reasons that will become clear later, we would like to give an idea of the proof of this theorem. The details can be found in [7]. The proof uses tools from the theory of diagrams of spaces. We will not go too much into the details, but let us recall that if $\mathcal{Q}$ is a poset, then $\mathcal{Q}$ can be seen as a category and a *simplicial $\mathcal{Q}$-diagram* is a functor from $\mathcal{Q}$ to the category of simplicial complexes.

If $f : \mathcal{P} \to \mathcal{Q}$ is a poset map, we let D be the $\mathcal{Q}$-diagram given by $D(q) = f^{-1}_{\leq q}$ and for $q' < q$, the morphism $d_{q',q} : f^{-1}_{\leq q'} \to f^{-1}_{\leq q}$ is the inclusion map. The first step in the proof of Theorem 2.8.1 is to prove the following lemma. This is done via the theory of arrangement of subspaces.

Lemma 2.8.2. *The poset $\mathcal{P}$ is homotopy equivalent to* $\operatorname{hocolim} D$.

As a second step, we consider the $\mathcal{Q}$-diagram E defined by $E(q) = f^{-1}_{\leq q}$ and with constant maps, i.e. if $q' < q$ then $e_{q',q}$ is the constant map sending every element of $f^{-1}_{\leq q'}$ to the chosen point $c_q \in f^{-1}_{\leq q}$. The following lemma follows then from the so-called Wedge Lemma (see for example [7, Lemma 2.2]).

Lemma 2.8.3.
$$\operatorname{hocolim} E \simeq \mathcal{Q} \vee \bigvee_{q \in \mathcal{Q}} \left(f^{-1}_{\leq q} * \mathcal{Q}_{>q} \right).$$

Remark 2.8.4. The proof of these two lemmas is independent of the assumption that the inclusion map $f^{-1}_{<q} \to f^{-1}_{\leq q}$ is homotopy equivalent to a constant map.

To prove the theorem, it only remains to show that $\operatorname{hocolim} D \simeq \operatorname{hocolim} E$. It is enough to show that there is a diagram map $\alpha : D \to E$ such that, for all $q \in \mathcal{Q}$, the map $\alpha_q : D(q) \to E(q)$ is a homotopy equivalence.

Suppose that $q \in \mathcal{Q}$ is not minimal. By the homotopy extension property for simplicial pairs, the homotopy from the inclusion map $f^{-1}_{<q} \hookrightarrow f^{-1}_{\leq q}$ to the constant map can be extended to a homotopy equivalence $\alpha_q : f^{-1}_{\leq q} \to \overline{f^{-1}_{\leq q}}$. For minimal $q \in Q$, the map α_q is the identity. This gives the desired diagram map $\alpha : D \to E$ and this finishes our sketch of the proof of Theorem 2.8.1.

In practice, given a poset map $f : \mathcal{P} \to \mathcal{Q}$, one can find more convenient conditions on the fibers to ensure that the inclusions $f^{-1}_{<q} \hookrightarrow f^{-1}_{\leq q}$ are homotopy equivalent to constant maps. This is the case, for example, if the fibers $f^{-1}_{\leq q}$ are sufficiently connected, as the next theorem shows.

Theorem 2.8.5 (Björner, Wachs, Welker)**.** *Let $f : \mathcal{P} \to \mathcal{Q}$ be a poset map such that for all $q \in \mathcal{Q}$ the fiber $f^{-1}_{\leq q}$ is $\dim(f^{-1}_{<q})$-connected. Then*
$$\mathcal{P} \simeq \mathcal{Q} \vee \bigvee_{q \in \mathcal{Q}} \left(f^{-1}_{\leq q} * \mathcal{Q}_{>q} \right).$$

For $q \in \mathcal{Q}$, we can write $f^{-1}_{<q} = \bigcup_{q'<q} f^{-1}_{\leq q'}$. In particular, if $f^{-1}_{\leq q}$ is r-connected and $f^{-1}_{\leq q'}$ has dimension at most r for all $q' < q$, then it follows by a standard topology argument that the inclusion map $f^{-1}_{<q} \hookrightarrow f^{-1}_{\leq q}$ is homotopy equivalent to a constant map. This observation was used by Pulkus and Welker in [22] in their study of $\mathcal{A}_p(G)$ for solvable groups G, and they obtain the following result.

Proposition 2.8.6. *Let $f : \mathcal{P} \to \mathcal{Q}$ be a poset map such that $f^{-1}_{\leq q}$ is spherical of dimension $d_q = \dim(f^{-1}_{\leq q})$, with $d_{q'} < d_q$ if $q' < q$. Then*
$$\mathcal{P} \simeq \mathcal{Q} \vee \bigvee_{q \in \mathcal{Q}} \left(f^{-1}_{\leq q} * \mathcal{Q}_{>q} \right).$$

Remark 2.8.7. If $f^{-1}_{\leq q}$ is r-connected, it is not enough to require that for each $q' < q$ the fiber $f^{-1}_{\leq q'}$ at most $r-1$-connected, since this does not imply necessarily that the union $f^{-1}_{<q} = \bigcup_{q'<q} f^{-1}_{\leq q'}$ is at most d-connected.

This proposition can be used to prove the following result of Quillen.

Proposition 2.8.8 (Quillen)**.** *Let $f : \mathcal{P} \to \mathcal{Q}$ be a poset map. Assume $\mathcal{Q}$ is d-spherical and for each $q \in \mathcal{Q}$ that $\mathcal{Q}_{>q}$ is $(d - h(q) - 1)$-spherical and $f^{-1}_{\leq q}$ is $h(q)$-spherical. Then $\mathcal{P}$ is d-spherical.*

Proof. By assumption $f^{-1}_{\leq q}$ is spherical of dimension $h(q) = \dim(f^{-1}_{\leq q}) = d_q$. Furthermore, if $q' < q$, then $h(q') < h(q)$ so that $d_{q'} < d_q$. Proposition 2.8.6 implies now

$$\mathcal{P} \simeq \mathcal{Q} \vee \bigvee_{q \in \mathcal{Q}} \left(f^{-1}_{\leq q} * \mathcal{Q}_{>q} \right). \tag{2.41}$$

Since $\mathcal{Q}_{>q}$ is spherical of dimension $d - h(q) - 1$, we have that $f^{-1}_{\leq q} * \mathcal{Q}_{>q}$ is spherical of dimension $(d - h(q) - 1) + h(q) + 1 = d$ (see 8.1 in [23]). Since $\mathcal{Q}$ is also d-spherical, we have that all the wedge summands in the right-hand side of equation (2.41) are spherical of dimension d. It follows that $\mathcal{P}$ is spherical of dimension d. □

It is not really the result that interests us here but more the method. In [23], Quillen' proof is based on the spectral sequence (2.33) and what we would like to point out here is that the two methods, namely the theory of diagrams and the spectral sequence, can yield the same result.

In the paper [12], Fumagalli makes the following assumptions on a poset map $f : \mathcal{P} \to \mathcal{Q}$ (see [12, Corollary 5]).

Assumption 1. *$\mathcal{Q}$ is a meet semi-lattice with unique least element $\hat{0}$;*

Assumption 2. *for every $q \in Q_{>\hat{0}}$, $f^{-1}_{\leq q} \supsetneq f^{-1}(\{\hat{0}\})$;*

Assumption 3. *for every $q \in \mathcal{Q}$, $f^{-1}_{\leq q}$ is either contractible or a wedge of n_q-dimensional spheres , with $0 \leq n_{q'} < n_q$ if $q' < q$ in $\mathcal{Q}$.*

Fumagalli claims that under these assumptions there is a homotopy equivalence

$$\mathcal{P} \simeq f^{-1}(\{\hat{0}\}) * \mathcal{Q}_{>\hat{0}} \vee \bigvee_{q \in \mathcal{Q}_{>\hat{0}}} \left(f^{-1}_{\leq q} * \mathcal{Q}_{>q} \right). \tag{2.42}$$

It is given as a corollary to the three standard lemmas, namely the so-called Projection Lemma [7, Lemma 2.3], Homotopy Lemma [7, Lemma 2.1] and Wedge Lemma [7, Lemma 2.2], but no detailed proof is given. It is also mentioned as a corollary to Theorem 2.8.1 (Theorem 2.5 in [7]) or [22, Corollary 2.4]. Unfortunately, as stated, this result is false and we will give counterexamples below. The absence of a detailed proof makes it difficult to point out where the mistake is. But in view of our previous discussion and especially the sketch of the proof of Theorem 2.8.1, it is almost certain that the problem comes from Assumption 3.

We will present now an example which satisfies the three assumptions but for which Formula (2.42) does not hold.

Example 2.8.9. Let $f : \mathcal{P} = Q \backslash \{z_1, \hat{0}\} \to \mathcal{Q}$ be the inclusion of posets defined by their Hasse diagrams in Figure 2.1.

The poset $\mathcal{Q}$ is a meet semi-lattice with least element $\hat{0}$, so that Assumption 1 is satisfied as well as Assumption 2, since $f^{-1}(\hat{0}) = \emptyset$ and for $q \in \mathcal{Q}_{>\hat{0}}$ the fiber $f^{-1}_{\leq q}$ is non-empty. The fiber $f^{-1}_{\leq q}$ is contractible for every $q \in \mathcal{Q}_{>\hat{0}}$, except for $q = z_1$ in which case $f^{-1}_{\leq z_1} = \{y_0, z_0\}$ is a sphere of dimension 0, hence Assumption 3 is also satisfied. However, the poset $\mathcal{P}$ is contractible, whereas the right-hand side of formula (2.42) contains the wedge summand $\mathcal{Q}_{>\hat{0}}$ which is homotopy equivalent to a sphere of dimension 1, thus formula (2.42) does not hold.

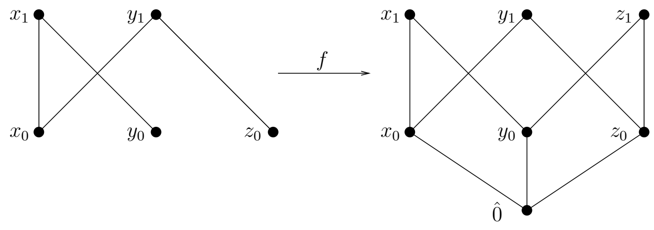

Figure 2.1: Hasse diagrams of $\mathcal{P}$ and $\mathcal{Q}$.

Note furthermore that the inclusion map $f^{-1}_{<z_1} \subseteq f^{-1}_{\leq z_1}$ is the identity map on $\{y_0, z_0\}$, hence is not homotopic to a constant map. Therefore, fiber theorems such as [22, Corollary 2.4] and [7, Theorem 2.5] don't apply.

We show how formula (2.42) is used by Fumagalli and provide a counterexample to the wedge decomposition he obtained along the proof of his Lemma 19. In his paper, Fumagalli introduces, for $X \in \mathcal{A}_p(G) \cup \{1\}$, the poset

$$\mathcal{M}_X(G) = \{U \in \mathcal{S}_p(G) \mid X < U,\, U = \Omega_1(U),\, \Phi(U) \leq X \leq Z(U)\}\,.$$

During the proof of [12, Lemma 19], he claims to prove the following formula: let A be a central elementary abelian p-subgroup of a finite group G, $1 \leq X \leq Y \leq A$ with $|Y : X| = p$ and let $R \leq A$ be such that $A = RY$ and $Y \cap R = X$. Fumagalli claims that under these assumptions, there is a homotopy equivalence

$$\mathcal{M}_X(G)_{>A} \simeq \mathcal{M}_Y(G)_{>A} \vee \bigvee_{U \in \mathcal{M}_Y(G)_{>A}} (\mathcal{A}_p(U/R)_{>A/R} * \mathcal{M}_Y(G)_{>U}). \quad (2.43)$$

Fumagalli obtains this formula by applying Formula (2.42) to the inclusion map $\mathcal{M}_X(G)_{>A} \hookrightarrow \mathcal{M}_Y(G)_{>A}$. We provide now a counterexample to Formula (2.43).

Example 2.8.10. Let p be an odd prime. We denote by P the p-group on the generators x_1, y_1, x_2, y_2, v, w of order p and with the commuting relations $[x_1, y_1] = [x_2, y_2] = w$, $[x_1, x_2] = v$ and all other commutators between generators trivial. Let $V = \langle v \rangle$ and $W = \langle w \rangle$. This group P has the following properties:

(i) $Z(P) = \langle v, w \rangle = V \times W$ is elementary abelian of rank 2;

(ii) $P' = \Phi(P) = Z(P)$;

(iii) P has exponent p;

(iv) P/V is extraspecial of order p^5 and exponent p with $Z(P/V) = Z(P)/V$.

For any subgroup H of P containing V, we will denote by $\overline{H}$ the quotient H/V. We would like to describe now Formula (2.43) in the following setting:

$$A = Z(P),\ X = \{1\},\ Y = V \text{ and } R = W.$$

In this situation, we can do the following identifications:

$$\mathcal{M}_X(P)_{>A} = \mathcal{A}_p(P)_{>Z(P)},\, \mathcal{M}_Y(P)_{>A} \cong \mathcal{A}_p(\overline{P})_{>Z(\overline{P})},$$

and for $B \in \mathcal{M}_Y(P)_{>A}$,

$$\mathcal{A}_p(B/R)_{>A/R} \cong \mathcal{A}_p(B)_{>Z(P)}.$$

Formula (2.43) is thus identical to the following formula:

$$\mathcal{A}_p(P)_{>Z(P)} \simeq \mathcal{A}_p(\overline{P})_{>Z(\overline{P})} \vee \bigvee_{\overline{B}=B/V\in\mathcal{A}_p(\overline{P})_{>Z(\overline{P})}} \left(\mathcal{A}_p(B)_{>Z(P)} * \mathcal{A}_p(\overline{P})_{>\overline{B}}\right). \tag{2.44}$$

Since $\overline{P}$ is extraspecial, we know from Lemma 2.3.15 that $\mathcal{A}_p(\overline{P})_{>Z(\overline{P})}$ is a wedge of p^4 spheres of dimension 1, so that the right-hand side of equation (2.44) is in particular not contractible. It turns out, however, that the left-hand side of equation (2.44), namely $\mathcal{A}_p(P)_{>Z(P)}$, is contractible.

To see this, we apply the Bouc-Thévenaz wedge decomposition to our group P defined above, with $A = Z(P)$ and $E_0 = \langle y_1, v, w\rangle$. In this situation, $M = C_P(E_0) = \langle y_1, x_2, y_2, v, w\rangle$ and the elementary abelian complements of M are of the form $F = \langle x_1x_2^r y_1^{s_1} y_2^{s_2}, v, w\rangle$. For such a complement, $C_M(F) = \langle y_1^{-r}y_2, v, w\rangle$ is elementary abelian, so that $\mathcal{A}_p(C_M(F))_{>A}$ is always contractible showing that $\mathcal{A}_p(P)_{>Z(P)}$ is contractible. It follows that Formula (2.44) does not hold and by extension Formula (2.43) does not hold in general.

Remark 2.8.11. Let p be an odd prime, P a p-group and let $A \in \mathcal{A}_p(P)_{>A}$. Let $X_0 = \{1\} \leq X_1 \leq \cdots \leq X_{r-1} \leq X_r = A$ be a chain of subgroups of A such that $|X_{i+1} : X_i| = p$. There are inclusion of posets

$$\mathcal{A}_p(P)_{>A} = \mathcal{M}_{\{1\}}(P)_{>A} \to \mathcal{M}_{X_1}(P)_{>A} \to \cdots \mathcal{M}_{X_{r-1}}(P)_{>A} \to \mathcal{M}_A(P).$$

The idea of Fumagalli was to apply Formula (2.43) recursively, in order to connect the homotopy type of $\mathcal{A}_p(P)_{>A}$ with the homotopy type of $\mathcal{M}_A(P)$. As we have seen in in Example 2.8.10, Formula (2.43) does not hold in general and as a consequence, the proof of Fumagalli's lemma 19 does not hold in general. This lemma 19 is a central argument in Fumgalli's main claim [12, Theorem 21], that $\mathcal{A}_p(G)$ has the homotopy type of a wedge of spheres for solvable groups G. As a consequence, whether $\mathcal{A}_p(G)$ is homotopy equivalent to a wedge of spheres for solvable groups G, seems to remain an open question.

As we have seen before with Proposition 2.8.8, some results can be proved using either fiber theorems or Quillen's spectral sequence. We have seen in Example 2.8.10 a situation for which fiber theorems don't apply and we will show now, in a special situation, what results can be obtained using Quillen's spectral sequence.

Let p be an odd prime number. Let P be a non-abelian p-group with $Z = \Omega_1(Z(P))$ of rank 2 and such that P/Z is elementary abelian. We wish to determine $\mathcal{A}_p(P)_{>Z}$, so that we may assume also that $P = \Omega_1(P)$, and in particular P has exponent p.

Let V, W be central subgroups of P of order p such that $Z = V \times W$, and let $\overline{P} = P/V$. For any subgroup H containing Z, we will denote by $\overline{H}$ the corresponding subgroup in $\overline{P}$. Since $\Phi(P) \leq Z$, we have in particular that $\Phi(\overline{P}) \leq \overline{Z}$ has order 1 or p. It follows now from Proposition 1.3.18 that $\overline{P}$ is isomorphic to a direct product $Q \times E$, where E elementary abelian of rank $m \geq 0$, and Q is either trivial, or extraspecial of type I, i.e. $Q = X_{p^{2\ell+1}}$ with $\ell \geq 0$.

Let $f : \mathcal{A}_p(P)_{>Z} \to \mathcal{A}_p(\overline{P})_{>\overline{Z}}$ be the poset map given by $f(A) = \overline{A}$. We determine first the fibers of f in the following lemma.

Lemma 2.8.12. *Let $\overline{B} = B/V \in \mathcal{A}_p(\overline{P})_{>\overline{Z}}$, then $f^{-1}_{\leq \overline{B}} = \mathcal{A}_p(B)_{>Z}$. Furthermore,*

a) If $h(\overline{B})$ is even, then $f^{-1}_{\leq \overline{B}}$ is contractible.

b) If $h(\overline{B})$ is odd, then $f^{-1}_{\leq \overline{B}}$ is either contractible, or has the homotopy type of a wedge of p^{k^2} spheres of dimension $\frac{h(\overline{B})-1}{2}$, where $k = \frac{h(\overline{B})+1}{2}$.

Proof. It follows directly from the definition of f that $f^{-1}_{\leq \overline{B}} = \mathcal{A}_p(B)_{>Z}$. If $Z(B) > Z$, then $Z(B) \in \mathcal{A}_p(B)_{>Z}$, since P has exponent p. Therefore, $\mathcal{A}_p(B)_{>Z}$ is conically contractible, via the inequalities

$$A \leq AZ(B) \geq Z(B), \text{ for all } A \in \mathcal{A}_p(B)_{>Z}.$$

We suppose from now on that $Z(B) = Z$. We have that $\overline{B} = B/V$ is elementary abelian, so that we can choose a complement B_0/V to Z/V in B/V, that is,

$$B/V = B_0/V \times Z/V.$$

We have thus $B_0 \cap Z = V$, so that $B_0 \cap W = 1$. Furthermore, B is generated by B_0 and $Z = V \times W$, hence by B_0 and W, since B_0 contains V. It follows then that $B = B_0 \times W$. Since V is central in B_0 and $V \times W = Z = Z(B) = Z(B_0) \times W$, we have $Z(B_0) = V$. Since B_0/V is elementary abelian, we have thus that B_0 is extraspecial of type I, i.e. $B_0 \cong X_{p^{2k+1}}$. Note that $k \geq 1$, since $B_0/V > Z/V$.

This shows in particular that B_0/V has even rank $2k$, and hence B/V has odd rank $2k+1$. Since $\overline{B}$ has height $\mathrm{rk}(B/V) - 1 = 2k$ in $\mathcal{A}_p(\overline{P})$, we have that $\overline{B}$ has height $2k-1$ in $\mathcal{A}_p(\overline{P})_{>\overline{Z}}$. This implies then that, for any $\overline{F} \in \mathcal{A}_p(\overline{P}_{>\overline{Z}})$, we have $Z(F) > Z$ if $h(\overline{F})$ is even, so that $f^{-1}_{\leq \overline{F}}$ is always contractible if $h(\overline{F})$ is even.

Since $Z(B_0) = V$ and $Z = V \times W$, the two posets $\mathcal{A}_p(B)_{>Z}$ and $\mathcal{A}_p(B_0)_{>Z(B_0)}$ are isomorphic. Since B_0 is isomorphic to $X_{p^{2k+1}}$, we have by Lemma 2.3.15, that $\mathcal{A}_p(B_0)_{>Z(B_0)}$ has the homotopy type of a wedge of p^{k^2} spheres of dimension $k-1$. The lemma follows now from the equality $k = \frac{h(\overline{B})+1}{2}$. □

Since $\overline{P}$ is isomorphic to $X_{p^{2\ell+1}} \times E$, with $\ell \geq 0$ and E elementary abelian of rank $m \geq 0$, we have from Lemma 2.5.9 and Lemma 2.5.11, that $\mathcal{A}_p(\overline{P})$ is hCM of dimension $d = \ell + (m-1) + 1 = \ell + m$, and hence $\mathcal{A}_p(\overline{P})_{>\overline{Z}}$ is hCM of dimension $\ell + m - 1$. We can apply now Quillen's spectral sequence (Proposition 2.7.1) to the map $f : \mathcal{A}_p(P)_{>Z} \to \mathcal{A}_p(\overline{P})_{>\overline{Z}}$. We have preferred however to extract the strictly needed informations on f, in order to give a general lemma on posets. Our purpose in doing so, is to ease notation.

Proposition 2.8.13. *Let $f : \mathcal{P} \to \mathcal{Q}$ be a poset map. We assume that $\mathcal{Q}$ is hCM of dimension $d \geq 0$ and we make the following assumptions on the fibers: If $h(q)$ is odd, then $f^{-1}_{\leq q}$ is either contractible, or has the homotopy type of a wedge of spheres of dimension $\frac{h(q)-1}{2}$, and if $h(q)$ is even, then $f^{-1}_{\leq q}$ is contractible. Then,*

a) If $d = 0$, then $\mathcal{P}$ is homotopy equivalent to $\mathcal{Q}$.

b) If $d = 1$, then $H_k(\mathcal{P}) = 0$ if $k \geq 2$ and there is an exact sequence

$$0 \to H_1(\mathcal{P}) \to H_1(\mathcal{Q}) \to \bigoplus_{h(q)=1} \left(\tilde{H}_{-1}(Q_{>q}) \otimes \tilde{H}_0(f^{-1}_{\leq q})\right) \to H_0(\mathcal{P}) \to \mathbb{Z} \to 0.$$

c) If $d > 1$, there is a spectral sequence E^2_{rs} converging to $H_{r+s}(\mathcal{P})$ with

$$E^2_{rs} = 0, \text{ if either } s > 0 \text{ and } r + 2s \neq d - 1, \text{ or } s = 0 \text{ and } r \notin \{d-1, d\}$$

and

$$E^2_{rs} \cong \bigoplus_{h(q)=2s+1} \tilde{H}_{d-2s-2}(\mathcal{Q}_{>q}) \otimes \tilde{H}_s(f^{-1}_{\leq q}), \text{ if } s > 0 \text{ and } r + 2s = d - 1.$$

Moreover, there is an exact sequence

$$0 \to E^2_{d,0} \to H_d(\mathcal{Q}) \to \bigoplus_{h(q)=1} \tilde{H}_{d-2}(\mathcal{Q}_{>q}) \otimes \tilde{H}_0(f^{-1}_{\leq q}) \to E^2_{d-1,0} \to 0.$$

In particular, the only non-zero terms are either $E^2_{d,0}$, or concentrated on the line $r + 2s = d - 1$ (which has the same direction as the differentials). Therefore, $E^\infty_{rs} = E^3_{rs}$.

Proof. Suppose first $d = 0$. In this situation, $\mathcal{Q}$ has no elements of odd height, so that by assumption, $f^{-1}_{\leq q}$ is contractible for all $q \in \mathcal{Q}$. It follows now from the Quillen fiber lemma that $\mathcal{P}$ and $\mathcal{Q}$ are homotopy equivalent.

We suppose from now on that $d \geq 1$. Recall from Proposition 2.7.1 that Quillen's spectral sequence has the following form, for any poset map $f : \mathcal{P} \to \mathcal{Q}$,

$$E^2_{rs} = H_r\left(\mathcal{Q}, q \mapsto H_s(f^{-1}_{\leq q})\right) \Rightarrow H_{r+s}(\mathcal{P}).$$

For $s > 0$, we have $\tilde{H}_s(f^{-1}_{\leq q}) = H_s(f^{-1}_{\leq q})$ for any $q \in \mathcal{Q}$, so that in this case,

$$E^2_{rs} = H_r\left(\mathcal{Q}, q \mapsto \tilde{H}_s(f^{-1}_{\leq q})\right). \tag{2.45}$$

For $s = 0$ there is an exact sequence

$$\cdots \to H_{r+1}(\mathcal{Q}) \to H_r\left(\mathcal{Q}, q \mapsto \tilde{H}_0(f^{-1}_{\leq q})\right) \to E^2_{r0} \to H_r(\mathcal{Q}) \to \cdots \tag{2.46}$$

associated to the short exact sequence

$$0 \to \tilde{H}_0(f^{-1}_{\leq q}) \to H_0(f^{-1}_{\leq q}) \to \mathbb{Z} \to 0.$$

We describe now these groups $H_r\left(\mathcal{Q}, q \mapsto \tilde{H}_s(f^{-1}_{\leq q})\right)$. Recall that if A is any abelian group, we denote $A_{(q)}$ the functor from $\mathcal{Q}$ to the category of abelian groups, sending q to A and all other elements of $\mathcal{Q}$ to 0. Let $s \geq 0$. By the assumptions made on the fibers, we have that $\tilde{H}_s(f^{-1}_{\leq q}) \neq 0$ implies $s = \frac{h(q)-1}{2}$. It follows that the functor $q \mapsto \tilde{H}_s(f^{-1}_{\leq q}) \neq 0$ is the direct sum of the functors $\tilde{H}_s(f^{-1}_{\leq q})_{(q)}$, where q ranges over all elements of $\mathcal{Q}$ of height $2s+1$. We have then

$$H_r\left(\mathcal{Q}, q \mapsto \tilde{H}_s(f^{-1}_{\leq q})\right) \cong \bigoplus_{h(q)=2s+1} H_r\left(\mathcal{Q}, \tilde{H}_s(f^{-1}_{\leq q})_{(q)}\right) \tag{2.47}$$

$$\cong \bigoplus_{h(q)=2s+1} \tilde{H}_{r-1}\left(\mathcal{Q}_{>q}, \tilde{H}_s(f^{-1}_{\leq q})\right), \tag{2.48}$$

where the second isomorphism comes from Lemma 2.6.7. Since $\mathcal{Q}$ is assumed to be hCM of dimension d, we have that $Q_{>q}$ is $(d-h(q)-1)$-spherical. It follows that

$$\tilde{H}_{r-1}\left(\mathcal{Q}_{>q}, \tilde{H}_s(f^{-1}_{\leq q})\right) = 0, \text{ if } r-1 \neq d-h(q)-1. \tag{2.49}$$

We have thus $H_r\left(\mathcal{Q}, q \mapsto \tilde{H}_s(f^{-1}_{\leq q})\right) = 0$, if $r-1 \neq d-(2s+1)-1$, i.e. $r+2s \neq d-1$. This, together with (2.45), shows that

$$E^2_{rs} = 0, \text{ if } s > 0 \text{ and } r+2s \neq d-1,$$

and

$$E^2_{rs} \cong \bigoplus_{h(q)=2s+1} \tilde{H}_{r-1}\left(\mathcal{Q}_{>q}, \tilde{H}_s(f^{-1}_{\leq q})\right), \text{ if } s > 0 \text{ and } r+2s = d-1.$$

The case $s=0$ is a little bit more complicated, but we still have from (2.48) and (2.49) that

$$H_r\left(\mathcal{Q}, q \mapsto \tilde{H}_0(f^{-1}_{\leq q})\right) = 0, \text{ if } r \neq d-1,$$

and

$$H_{d-1}\left(\mathcal{Q}, q \mapsto \tilde{H}_0(f^{-1}_{\leq q})\right) \cong \bigoplus_{h(q)=1} \tilde{H}_{d-2}\left(\mathcal{Q}_{>q}, \tilde{H}_s(f^{-1}_{\leq q})\right). \tag{2.50}$$

Since $\mathcal{Q}$ is hCM of dimension d, we know furthermore that $H_k(\mathcal{Q}) =$ if $k \geq 1$ and $k \neq d$. We can enter now these informations into the long exact sequence (2.46).

Suppose first $d=1$. The long exact sequence (2.46) becomes

$$0 \to E^2_{1,0} \to H_1(\mathcal{Q}) \to H_0(\mathcal{Q}, q \mapsto \tilde{H}_0(f^{-1}_{\leq q})) \to E^2_{00} \to \mathbb{Z} \to 0. \tag{2.51}$$

Since $E^2_{rs} = 0$ if $s > 0$ and $r+2s \neq d-1 = 0$, we have $E^2_{rs} = 0$ for all $s > 0$. It follows that the only non-zero terms of E^2_{rs} are $E^2_{0,0}$ and $E^2_{1,0}$. In particular, $E^2_{rs} = E^\infty_{rs}$, so that $H_0(\mathcal{P}) = E^2_{0,0}$, $H_1(\mathcal{P}) = E^2_{1,0}$ and $H_k(\mathcal{P}) = 0$ if $k > 1$. The exact sequence (2.51) can now be rewritten

$$0 \to H_1(\mathcal{P}) \to H_1(\mathcal{Q}) \to \bigoplus_{h(q)=1} \tilde{H}_{-1}\left(Q_{>q}, \tilde{H}_0(f^{-1}_{\leq q})\right) \to H_0(\mathcal{P}) \to \mathbb{Z} \to 0.$$

The result for $d = 1$ will now follow from the isomorphism given in (2.52) below.

Suppose now $d > 1$. The long exact sequence (2.46) becomes

$$0 \to E^2_{d,0} \to H_d(\mathcal{Q}) \to H_{d-1}(\mathcal{Q}, q \mapsto \tilde{H}_0(f^{-1}_{\leq q})) \to E^2_{d-1,0} \to 0.$$

This shows in particular that the non-zero terms of E^2_{rs} are concentrated on the diagonal $r + 2s = d - 1$ and on $E^2_{d,0}$. As a consequence, the spectral sequence converges at the third page, i.e. $E^3_{rs} = E^\infty_{rs}$. The proposition follows now from (2.50) and the following isomorphism, coming from the fact that the top homology of a spherical complex is free,

$$\tilde{H}_{r-1}\left(\mathcal{Q}_{>q}, \tilde{H}_s(f^{-1}_{\leq q})\right) \cong \tilde{H}_{r-1}(\mathcal{Q}_{>q}) \otimes \tilde{H}_s(f^{-1}_{\leq q}). \tag{2.52}$$

□

Remark 2.8.14. Consider the exact sequence coming from the previous proposition:

$$0 \to E^2_{d,0} \to H_d(\mathcal{Q}) \to \bigoplus_{h(q)=1} \tilde{H}_{d-2}\left(\mathcal{Q}_{>q}, \tilde{H}_s(f^{-1}_{\leq q})\right) \to E^2_{d-1,0} \to 0.$$

The homomorphism

$$H_d(\mathcal{Q}) \to \bigoplus_{h(q)=1} \tilde{H}_{d-2}\left(\mathcal{Q}_{>q}, \tilde{H}_s(f^{-1}_{\leq q})\right)$$

in this exact sequence comes from the connecting homomorphism $H_d(\mathcal{Q}) \to H_{d-1}(Q, q \mapsto \tilde{H}_0(f^{-1}_{\leq q}))$. If this homomorphism is zero, then the exact sequence splits into two sequences

$$0 \to E^2_{d,0} \to H_d(\mathcal{Q}) \to 0$$

and

$$0 \to \bigoplus_{h(q)=1} \tilde{H}_{d-2}\left(\mathcal{Q}_{>q}, \tilde{H}_s(f^{-1}_{\leq q})\right) \to E^2_{d-1,0} \to 0.$$

In this situation, we would have in particular $H_d(\mathcal{P}) = E^2_{d,0} = H_d(\mathcal{Q})$. There are unfortunately situations in which this homomorphism is not zero (see Example 2.8.16).

We return now to the situation of our p-group above. Recall that p is an odd prime number and that P is a non-abelian p-group with $Z = \Omega_1(Z(P))$ of rank 2 and such that P/Z is elementary abelian. Without loss of generality, we suppose also that P has exponent p.

Recall also that V, W are central subgroups of P of order p such that $Z = V \times W$ and we denote by $\overline{P}$ the quotient P/V. For any subgroup H containing Z, we denote by $\overline{H}$ the corresponding subgroup in $\overline{P}$. Recall that $\overline{P}$ is isomorphic to $E \times X_{p^{2\ell+1}}$, with E elementary abelian of rank $m \geq 0$ and $\ell \geq 0$. In particular, $\mathcal{A}_p(\overline{P})$ is hCM of dimension $d = \ell + r - 2$ and in view of Lemma 2.8.12, we can apply Proposition 2.8.13 to the map $f : \mathcal{A}_p(P)_{>Z} \to \mathcal{A}_p(\overline{P})_{\overline{Z}}$. To save some space, we will not write down explicitly the result obtained, but we wiil do some examples instead. These examples will show in particular that there are non-trivial differentials to handle, so that this spectral sequence may not be very easy to use for calculations.

Example 2.8.15. If $\ell = 0$, then $\overline{P} = P/V$ is elementary abelian of rank m. It follows that $\Phi(P) = V$ and has order p. The fact that $Z = \Omega_1(Z(P))$ has rank 2 and Proposition 1.3.18 imply that $P = Q \times U$, with $Q \cong X_{p^{2k+1}}$ and $\Phi(Q) = V$. Of course, it is easy now to compute the homotopy type of $\mathcal{A}_p(P)_{>Z}$. Indeed, we have $\mathcal{A}_p(P)_{>Z} \cong \mathcal{A}_p(Q)_{>Z(Q)}$, which is spherical of dimension $k-1$ (see Lemma 2.3.15). It is not difficult to see that the results obtained by applying Proposition 2.8.13 are consistent with this result.

Example 2.8.16. In this example, we apply Proposition 2.8.13 to the group P defined in Example 2.8.10. Recall that p is an odd prime and P is the p-group with generators x_1, y_1, x_2, y_2, v, w of order p and with commuting relations $[x_1, y_1] = [x_2, y_2] = w$ and $[x_1, x_2] = v$. All other commutators between generators are trivial. Let $V = \langle v \rangle$ and $W = \langle w \rangle$, so that $Z = \Omega_1(Z(P)) = Z(P) = V \times W$. Furthermore, $\overline{P} = P/Z$ is isomorphic to X_{p^5}, so that here $\ell = 2$ and $m = 0$. In particular, $\mathcal{A}_p(\overline{P})_{>\overline{Z}}$ is hCM of dimension $d = \ell + m - 1 = 1$.

Proposition 2.8.13 implies that $H_k(\mathcal{A}_p(P)_{>Z}) = 0$ for $k \geq 2$ and that there is an exact sequence

$$\begin{aligned} 0 \to H_1(\mathcal{A}_p(P)_{>Z}) &\to H_1(\mathcal{A}_p(\overline{P})_{>\overline{Z}}) \\ &\to \bigoplus_{\substack{\overline{B} \in \mathcal{A}_p(\overline{P})_{>\overline{Z}} \\ \mathrm{rk}(\overline{B})=3}} \tilde{H}_0(\mathcal{A}_p(B)_{>Z}) \to H_0(\mathcal{A}_p(P)_{>Z}) \to \mathbb{Z} \to 0. \end{aligned} \tag{2.53}$$

We have used here the fact that if $\overline{B} = B/V$ has height 1 in $\mathcal{A}_p(\overline{P})_{>\overline{Z}}$, then $\overline{B}$ has rank 3. In this case, $\mathcal{A}_p(\overline{P})_{>\overline{B}}$ is empty, so that $\tilde{H}_{-1}(\mathcal{A}_p(\overline{P})_{>\overline{B}}) = \mathbb{Z}$. Furthermore, $\tilde{H}_0(\mathcal{A}_p(B)_{>Z})$ is non-zero if and only if $B = B_0 \times B$, with $B_0 \cong X_{p^3}$ and $Z(B_0) = V$. In this case, $\mathcal{A}_p(B)_{>Z} \cong \mathcal{A}_p(B_0)_{>V}$ is a wedge of p spheres of dimension 0. Such subgroups B exist and we can consider for example the subgroup $B = \langle x_1, x_2, v, w \rangle$, in which case $B_0 = \langle x_1, x_2, v \rangle$. There are p^3 such subgroups in P, so that

$$\bigoplus_{\substack{\overline{B} \in \mathcal{A}_p(\overline{P})_{>\overline{Z}} \\ \mathrm{rk}(\overline{B})=3}} \tilde{H}_0(\mathcal{A}_p(B)_{>Z}) \cong \bigoplus_{p^3} \mathbb{Z}^p = \mathbb{Z}^{p^4}.$$

Furthermore, since $\overline{P} = X_{p^5}$, we have that $\mathcal{A}_p(\overline{P})_{>\overline{Z}}$ has the homotopy type of a wedge of p^4 spheres of dimension 1, hence $H_1(\mathcal{A}_p(\overline{P})_{>\overline{Z}})\mathbb{Z}^{p^4}$. The exact sequence (2.53) can now be rewritten

$$0 \to H_1(\mathcal{A}_p(P)_{>Z}) \to \mathbb{Z}^{p^4} \to \mathbb{Z}^{p^4} \to H_0(\mathcal{A}_p(P)_{>Z}) \to \mathbb{Z} \to 0$$

This exact sequence is however not sufficient to determine the homology groups of $\mathcal{A}_p(P)_{>Z}$, without the knowledge of the homomorphism $\mathbb{Z}^{p^4} \to \mathbb{Z}^{p^4}$.

Using the Bouc-Thévenaz Wedge Decomposition Formula, we have seen however in Example 2.8.10, that $\mathcal{A}_p(P)_{>Z}$ is in fact contractible. The exact sequence (2.53) has thus the following form:

$$0 \to 0 \to \mathbb{Z}^{p^4} \to \mathbb{Z}^{p^4} \to \mathbb{Z} \to \mathbb{Z} \to 0.$$

In particular, the connecting homomorphism $\mathbb{Z}^{p^4} \to \mathbb{Z}^{p^4}$ is the identity.

Example 2.8.17. Let P be the group defined in the preceeding example. Let Q be defined as an iterated central products of this group P with itself. It is not difficult to see that, in this situation, there may be non-trivial terms on the diagonal of the spectral sequence obtained in Proposition 2.8.13. For such groups Q, however, the poset $\mathcal{A}_p(Q)_{>Z}$ is contractible. The differentials must thus be non-trivial in this situation.

Chapter 3

Automorphisms

In this chapter, we determine the automorphism groups for the following groups:

(I) p-groups with a cyclic Frattini subgroup.

(II) odd order p-groups of class 2 with a cyclic center and such that the quotient by the center is homocyclic.

3.1 Introduction

The purpose of this chapter is to describe the automorphism group of p-groups introduced in Chapter 1. To begin, we will consider p-groups with a cyclic Frattini subgroup. As was seen in the first chapter, such a group can be decomposed as $P = Q \times E$ where E is elementary abelian and Q has a cyclic center and a cyclic Frattini subgroup. The first step will be to get rid of the direct factor E. This will be done by using work of Bidwell, Curran and McCaughan [5] on automorphism groups of direct product of groups with no common direct factor. We will then be able to assume that the center of P is cyclic. This will greatly simplify the proofs and the statement will also become more readable.

If the Frattini subgroup is central, that is, P is quasi-extraspecial in our terminology, we can then adapt the method used by Winter [32] to determine the automorphism group of extraspecial p-groups. We will first reduce the problem to the study of automorphisms fixing the center pointwise. We will then show that there is an exact sequence

$$1 \to \mathrm{Int}(P) \to \mathrm{Aut}_{Z(P)}(P) \to S \to 1,$$

where S is a (known) subgroup of a symplectic group.

When the Frattini subgroup of P is cyclic but is not central (and then $p = 2$), the method goes roughly as follows. Thanks to the work of Bidwell, Curran and Mc-Caughan, we may assume that $Z(P)$ is cyclic. Recall from Lemma 1.3.35 that $C_0 = C_P(\Phi(P))$ is then maximal in P and $\Phi(C_0) = \Phi(P)$ is central in C_0. We will then express $\mathrm{Aut}(P)$ in terms of automorphimsms of C_0.

The case of p-groups with central and cyclic Frattini subgroup can be generalized for the odd order p-groups of class 2 with cyclic center and such that $P/Z(P)$ is homocyclic. This will be done in Section 3.5.

3.2 Preliminaries and notation

Let G be a group and let C be a characteristic subgroup of G. The restriction of automorphisms induces a homomorphism

$$\rho_C : \mathrm{Aut}(G) \to \mathrm{Aut}(C).$$

We let $\mathrm{Aut}_C(G) = \ker \rho_C$. This is the normal subgroup of $\mathrm{Aut}(G)$ consisting of all automorphisms of G that restrict to the identity on C. If H is any subgroup in G, we denote similarly by $\mathrm{Aut}_H(G)$ the subgroup of $\mathrm{Aut}(G)$ consisting of automorphisms of G acting as the identity on H, that is

$$\mathrm{Aut}_H(G) = \{\alpha \in \mathrm{Aut}(G) \,|\, \alpha(h) = h, \forall h \in H\}.$$

Note that if H is not characteristic in G, then the subgroup $\mathrm{Aut}_H(G)$ is not necessarily normal in $\mathrm{Aut}(G)$.

Any automorphism α of G induces an automorphism $\overline{\alpha}$ on the quotient group G/C by $\overline{\alpha}(\overline{g}) = \overline{\alpha(g)}$ for all $\overline{g} \in G/C$. This defines a homomorphism

$$\pi_{G/C} : \mathrm{Aut}(G) \to \mathrm{Aut}(G/C).$$

We let $\mathrm{Aut}_{G/C}(G) = \ker \pi_{G/C}$. This is the normal subgroup of $\mathrm{Aut}(G)$ consisting of automorphisms of G inducing the identity on G/C.

We denote by $\mathrm{Aut}_{C,G/C}(G) = \mathrm{Aut}_C(G) \cap \mathrm{Aut}_{G/C}(G)$. This group can be seen as the kernel of the homomorphism

$$\mathrm{Aut}_C(G) \to \mathrm{Aut}(G/C)$$

given by the composition of the inclusion $\mathrm{Aut}_C(G) \hookrightarrow \mathrm{Aut}(G)$ followed by $\pi_{G/C} : \mathrm{Aut}(G) \to \mathrm{Aut}(G/C)$. This is the normal subgroup of $\mathrm{Aut}(G)$ consisting of all automorphisms of G that are the identity on C and that induce the identity on G/C. The following lemma gives a useful description of this group if C is also assumed to be central.

Lemma 3.2.1. *Let Z be a central and characteristic subgroup of a group G. Then $\mathrm{Aut}_{Z,G/Z}(G)$ is isomorphic to $\mathrm{Hom}(G/Z, Z)$.*

Proof. Remark first that $\mathrm{Hom}(G/Z, Z)$ is a group since Z is central in G. More precisely, for $\theta_1, \theta_2 \in \mathrm{Hom}(G/Z, Z)$, the product $\theta_1\theta_2$ is defined by $(\theta_1\theta_2)(\overline{g}) = \theta_1(\overline{g})\theta_2(\overline{g})$ for all $\overline{g} \in G/Z$.

If θ is a homomorphism from G/Z to Z, we define $f(\theta) : G \to G$ by $f(\theta)(g) = \theta(\overline{g})g$ for all $g \in G$. Since Z is central in G, we have that $f(\theta)$ is a homomorphism. If $f(\theta)(g) = 1$, then $\theta(\overline{g})g = 1$ and hence g must be in Z. But then $\theta(\overline{g}) = 1$, so that $1 = f(\theta)(g) = g$. This shows that $f(\theta)$ is injective and thus is an automorphism of G since G is finite. Furthermore, it is clear from the definition that $f(\theta)$ fixes Z pointwise and induces the identity on G/Z.

We have thus a map $f : \mathrm{Hom}(G/Z, Z) \to \mathrm{Aut}_{Z,G/Z}(G)$ and f turns out to be a homomorphism since

$$f(\theta_1\theta_2)(g) = \theta_1(\overline{g})\theta_2(\overline{g})g = f(\theta_1)(\theta_2(\overline{g})g) = f(\theta_1)(f(\theta_2)(g)).$$

If $f(\theta)$ is the identity on G, then $g = f(\theta)(g) = \theta(\overline{g})g$. It follows that $\theta(\overline{g}) = 1$ for all $\overline{g} \in G/Z$ and thus $\theta = 1$, showing that f is actually injective.

To see that f is also surjective, let $\rho \in \mathrm{Aut}_{Z,G/Z}(G)$. We have then $\overline{\rho(g)} = \overline{g}$ so that there exists a unique element $z_g \in Z$ such that $\rho(g) = gz_g$. Since θ is the identity on Z, we have $\rho(gz') = \rho(g)\rho(z') = \rho(g)z'$ and it follows that $z_g = z_{gz'}$ for all $z' \in Z$. There is thus a well-defined map $h(\rho) : G/Z \to Z$ by $h(\rho)(\overline{g}) = z_g$. It is not difficult to see that $h(\rho)$ is a homomorphism and that $f(h(\rho)) = \rho$. $\square$

For $g \in G$, we denote by c_g the inner automorphism of G given by conjugation by g, that is $c_g(x) = gxg^{-1}$. We denote by $\mathrm{Int}\, G = \{c_g \,|\, g \in G\}$ the group of inner automorphisms of G. If H is a subgroup of G, we denote $\mathrm{Int}_H\, G = \mathrm{Int}(G) \cap \mathrm{Aut}_H\, G$. We will also denote by $\mathrm{Int}(G, H)$ the subgroup of $\mathrm{Int}(G)$ generated by the inner automorphisms given by elements in H, that is $\mathrm{Int}(G, H) = \{c_h \,|\, h \in H\}$. Note that in general $\mathrm{Int}(G, H) \ncong \mathrm{Int}(H)$.

Lemma 3.2.2.

a) *For any $g \in G$ and $\alpha \in \mathrm{Aut}(G)$, one has $\alpha c_g \alpha^{-1} = c_{\alpha(g)}$. In particular, $\mathrm{Int}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.*

b) *The homomorphism sending $g \in G$ to $c_g \in \mathrm{Int}(G)$ induces an isomorphism $G/Z(G) \cong \mathrm{Int}(G)$.*

c) *If H is a subgroup of G, then $\mathrm{Int}(G, H) \cong H/(Z(G) \cap H)$.*

We will often make use of particular automorphisms of cyclic groups so that we fix some notation.

Notation 3.2.3. Let $C_n = \langle x \rangle$ be a cyclic group of order p^n, $n \geq 1$.

a) If p is odd, recall that $\mathrm{Aut}(C_n)$ is cyclic of order $p^{n-1}(p-1)$. We denote by θ the automorphism of C_n of order p defined by $\theta(x) = x^{1+p^{n-1}}$.

b) If $p = 2$ we denote similarly by θ the automorphism of C_n of order 2 defined by $\theta(x) = x^{1+2^{n-1}}$. We denote by τ the automorphism of C_n of order 2 given by $\tau(x) = x^{-1}$. Remark that if $n = 2$ then $\theta = \tau$ and $\mathrm{Aut}(C_2)$ is cyclic of order 2 and generated by τ and if $n > 2$ then $\mathrm{Aut}(C_n)$ is abelian of type $(2^{n-2}, 2)$ and θ and τ form a basis of $\Omega_1(\mathrm{Aut}(C_n))$.

Definition 3.2.4. We say that the short exact sequence $1 \to N \to G \xrightarrow{\pi} K \to 1$ splits if there exists homomorphism $r : K \to G$ such that $\pi r = \mathrm{id}_K$. We will call the homomorphism r a homomorphic section of π.

Lemma 3.2.5. *Let $\langle x \rangle$ be a cyclic group of order p^{m+1}, with $m \geq 1$, and let $\langle x^p \rangle$ be its unique maximal subgroup. Let θ be the automorphism of $\langle x \rangle$ defined by $\theta(x) = x^{1+p^m}$. Then the following sequence is exact:*

$$1 \to \langle \theta \rangle \to \mathrm{Aut}(\langle x \rangle) \xrightarrow{\rho_{\langle x^p \rangle}} \mathrm{Aut}(\langle x^p \rangle) \to 1$$

Furthermore,

a) *If p is odd, this sequence splits if and only if $m = 1$.*

b) *If $p = 2$, this sequence splits if and only if $m = 1$ or $m = 2$.*

Proof. On the one hand, we have $\theta(x^p) = (x^{1+p^m})^p = x^p x^{p^{m+1}} = x^p$, so that θ is in $\ker \rho_{\langle x^p \rangle}$. On the other hand, if α is an element of $\mathrm{Aut}(\langle x \rangle)$ then $\alpha(x) = x^k$ for some k prime to p. Therefore, if α is the identity on $\langle x^p \rangle$ we have

$$x^p = \alpha(x^p) = (\alpha(x))^p = (x^k)^p = (x^p)^k.$$

Since x^p has order p^m, it follows that $k \equiv 1 \mod p^m$, i.e. $k = 1 + ap^m$ for some a. But then $\alpha = \theta^a$ and this proves that $\ker \rho_{\langle x^p \rangle} = \langle \theta \rangle$.

It follows from the description of the automorphism groups of cyclic groups that $|\mathrm{Aut}(\langle x \rangle)| = p \cdot |\mathrm{Aut}(\langle x^p \rangle)|$, so that $\rho_{\langle x^p \rangle}$ must be surjective and this proves that the sequence is exact.

For the splitting, one has to consider separately the case p odd and $p = 2$. We suppose first that p is odd. If $m = 1$, then $\mathrm{Aut}(\langle x \rangle)$ is abelian of type $(p, p-1)$ and $\mathrm{Aut}(\langle x^p \rangle)$ has order $p-1$. Hence $\mathrm{Aut}(\langle x \rangle) = \langle \theta \rangle \times \mathrm{Aut}(\langle x^p \rangle)$ and the sequence splits.

When $m > 1$, the exact sequence becomes

$$1 \to C_p \to C_{p^{m-1}} \times C_{p-1} \to C_{p^{m-2}} \times C_{p-1} \to 1.$$

This sequence cannot split since $C_{p^{m-1}} \times C_{p-1}$ is not isomorphic $C_p \times C_{p^{m-2}} \times C_{p-1}$.

We suppose now $p = 2$. If $m = 1$, then $\mathrm{Aut}(\langle x^2 \rangle)$ is reduced to the identity so that the sequence trivially splits. If $m = 2$, $\mathrm{Aut}(\langle x \rangle)$ is elementary abelian of rank 2 and generated by θ and the involution τ sending x to x^{-1}. The group $\mathrm{Aut}(\langle x^2 \rangle)$ is cyclic of order 2 generated by the involution $x \mapsto x^{-1}$ which is the restriction of τ so that the sequence splits.

An argument similar to the one for p odd shows that the sequence does not split when $m > 2$. $\square$

Lemma 3.2.6. *Let G, G_1, G_2 be groups and suppose that the following diagram is commutative and the two rows are exact.*

$$\begin{tikzcd}
1 \arrow[r] & \ker f_1 \arrow[r] \arrow[d] & G \arrow[r, "f_1"] \arrow[d, equal] & G_1 \arrow[r] \arrow[d, "g"] & 1 \\
1 \arrow[r] & \ker f_2 \arrow[r] & G \arrow[r, "f_2"] & G_2 \arrow[r] & 1
\end{tikzcd}$$

Then

a) $\ker f_2 / \ker f_1 \cong \ker g$.

b) If f_2 splits then g splits.

c) If g and f_1 split, then f_2 splits.

d) If f_1 splits, then $\ker f_2 \cong \ker f_1 \rtimes \ker g$.

We recall finally some standard notation and results on symplectic and orthogonal groups. More details can be found in Chapter 8 and Chapter 11 of Taylors's book [28].

Let $\mathbb{F}$ be a field and let V be a vector space over $\mathbb{F}$. If $b : V \times V \to \mathbb{F}$ is an alternating form on V, we denote $Sp(V)$ the subgroup of $GL(V)$ consisting of linear transformations of V preserving b, namely

$$Sp(V) = \{\sigma \in GL(V) \,|\, b(\sigma v, \sigma w) = b(v, w),\, \forall v, w \in V\}\,.$$

If the alternating form b is non-degenerate, then V has even dimension 2ℓ for some $\ell \geq 1$ and has a basis such that the matrix of b relatively to this basis is given by

$$B = \begin{pmatrix} 0 & I_\ell \\ -I_\ell & 0 \end{pmatrix}.$$

The group $Sp(V)$ is then isomorphic to the subgroup $Sp(2\ell, \mathbb{F})$ of $GL_{2\ell}(\mathbb{F})$ consisting of invertible matrices such that $ABA^t = B$. When $\mathbb{F}$ is the finite field $\mathbb{F}_p$, we will denote by $Sp(2\ell, p)$ the group $Sp(2\ell, \mathbb{F}_p)$.

Lemma 3.2.7.

$$|Sp(2\ell, p)| = p^{\ell^2} \prod_{i=1}^{\ell} (p^{2i} - 1)$$

Suppose from now on that $\mathbb{F}$ is a finite field of characteristic 2 and let $q : V \to \mathbb{F}$ be a quadratic form on V. The orthogonal group of q is the subgroup $O(V, q)$ (or simply $O(V)$) of $GL(V)$ consisting of linear transformations of V preserving q, namely

$$O(V, q) = \{\sigma \in GL(V) \,|\, q(\sigma v) = q(v)\, \forall v \in V\}\,.$$

The polar form b on q is the alternating form defined by $b(v, w) = q(v + w) - q(v) - q(w)$ and the form q is non-degenerate if $V^\perp$ has no singular vectors, i.e. $q(w) \neq 0$, for all $w \in V^\perp$. If V has odd dimension $2\ell + 1$, there is only one non-degenerate quadratic form on V up to isomorphism and we denote $O(2\ell + 1, \mathbb{F})$ the corresponding orthogonal group. If V has even dimension 2ℓ, there are two non-isomorphic non-degenerate quadratic q^+, q^- form on q. We denote by $O^+(2\ell, \mathbb{F})$ and $O^-(2\ell, \mathbb{F})$ the two corresponding (non-isomorphic) orthogonal groups $O(V)$ (see [28, Chapter 11] for details).

Similarly to the case of symplectic groups, we use the respective notation $O(2\ell + 1, 2)$, $O^+(2\ell, 2)$, $O^-(2\ell, 2)$ when $\mathbb{F}$ is the field $\mathbb{F}_2$.

3.3 Automorphisms of direct products of groups

In this section, we recall briefly the results of Bidwell, Curran and McCaughan on automorphisms of direct products of groups with no common direct factor. For the proofs, the reader is referred to [5].

Let G, H be finite groups. If $\theta, \psi \in \mathrm{Hom}(G, H)$, the map $\theta + \psi : G \to H$ defined by $(\theta + \psi)(g) = \theta(g)\psi(g)$ is again a homomorphism if $\mathrm{Im}\,\theta$ and $\mathrm{Im}\,\psi$ commute.

Definition 3.3.1. Let $G = H \times K$, we define

$$\mathcal{E} = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \begin{array}{lll} \alpha \in \mathrm{End}(H), & \beta \in \mathrm{Hom}(K, H), & [\mathrm{Im}\,\alpha, \mathrm{Im}\,\beta] = 1, \\ \gamma \in \mathrm{Hom}(H, K), & \delta \in \mathrm{End}(K), & [\mathrm{Im}\,\gamma, \mathrm{Im}\,\delta] = 1. \end{array} \right\}$$

The set $\mathcal{E}$ is a monoid under matrix multiplication

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' + \beta\gamma' & \alpha\beta' + \beta\delta' \\ \gamma\alpha' + \delta\gamma' & \gamma\beta' + \delta\delta' \end{pmatrix}$$

Proposition 3.3.2 (Bidwell-Curran-McCaughan)**.** *If* $G = H \times K$, *then* $\mathrm{End}(G)$ *is isomorphic to* $\mathcal{E}$.

Proof. See Bidwell-Curran-McCaughan [5] □

Definition 3.3.3. Let $G = H \times K$ and let

$$\mathcal{A} = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \begin{array}{ll} \alpha \in \mathrm{Aut}(H), & \beta \in \mathrm{Hom}(K, Z(H)), \\ \gamma \in \mathrm{Hom}(H, Z(K)), & \delta \in \mathrm{Aut}(K), \end{array} \right\} \subseteq \mathcal{E}$$

Proposition 3.3.4 (Bidwell-Curran-McCaughan)**.** *Let* $G = H \times K$ *where* H *and* K *have no common direct factor, then* $\mathrm{Aut}(G) \cong \mathcal{A}$.

Proof. See [5]. □

Corollary 3.3.5. *Let* $G = H \times K$, *where* H *and* K *have no common direct factor, then*

$$|\mathrm{Aut}(G)| = |\mathrm{Aut}(H)| \cdot |\mathrm{Aut}(K)| \cdot |\mathrm{Hom}(H, Z(K))| \cdot |\mathrm{Hom}(K, Z(H))|$$

3.4 Automorphisms of p-groups with cyclic Frattini subgroup

Let p be an arbitrary prime and let P be a p-group with cyclic Frattini subgroup. We know from Lemma 1.3.2 that $P = Q \times E$ with E elementary abelian and Q has a cyclic center and $\Phi(Q) = \Phi(P)$ is cyclic. In particular, Q and E have no common direct factor and Proposition 3.3.4 gives the following result.

Lemma 3.4.1. *Let* $P = Q \times E$ *be a* p*-group with* E *elementary abelian and such that* Q *has a cyclic Frattini subgroup and a cyclic center. Then* $\mathrm{Aut}(P)$ *is isomorphic to the group*

$$\mathcal{A} = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \begin{array}{ll} \alpha \in \mathrm{Aut}(Q), & \beta \in \mathrm{Hom}(E, Z(Q)), \\ \gamma \in \mathrm{Hom}(Q, Z(E)), & \delta \in \mathrm{Aut}(E), \end{array} \right\}.$$

Lemma 3.4.2. *Let* $P = Q \times E$ *be a* p*-group with* E *elementary abelian and such that* Q *has a cyclic Frattini subgroup and a cyclic center. Let* d *denote the* p*-rank of* $Q/\Phi(Q)$ *and let* r *be the* p*-rank of* $Z(P)$.

a) $\mathrm{Aut}(E)$ *is isomorphic to* $GL_{r-1}(\mathbb{F}_p)$*,*

b) $\mathrm{Hom}(E, Z(Q))$ *is an elementary abelian p-group of rank* $r-1$*,*

c) $\mathrm{Hom}(Q, Z(E)) = \mathrm{Hom}(Q, E)$ *is isomorphic to the group* $M_{(r-1)\times d}(\mathbb{F}_p)$ *of* $(r-1)\times d$ *matrices.*

Proof.

a) The group E is elementary abelian of rank $r-1$, hence can be viewed as an $\mathbb{F}_p$-vector space of dimension $r-1$. Choosing a basis, we can identify its automorphism group with the group $GL_{r-1}(\mathbb{F}_p)$.

b) Let Z be the unique subgroup of order p of $Z(Q)$. Since E is elementary abelian, $\mathrm{Hom}(E, Z(Q)) = \mathrm{Hom}(E, Z) \cong E$.

c) Since E is elementary abelian we have

$$\mathrm{Hom}(Q, Z(E)) = \mathrm{Hom}(Q, E) = \mathrm{Hom}(Q/\Phi(Q), E).$$

Choosing a basis of $Q/\Phi(Q)$ and a basis of E, we can identify the group $\mathrm{Hom}(Q/\Phi(Q), E)$ with the group of $(r-1)\times d$ matrices with coefficients in $\mathbb{F}_p$.

□

Corollary 3.4.3. *If* $P = Q \times E$ *where* E *is elementary abelian of rank* $r-1$ *and* Q *has a cyclic center and a cyclic Frattini subgroup, then*

$$|\,\mathrm{Aut}(P)| = |\,\mathrm{Aut}(Q)| \cdot p^a \prod_{i=1}^{r-1}(p^i - 1)$$

where $a = \frac{r(r-1)}{2} + d(r-1)$*.*

It remains thus to determine $\mathrm{Aut}(Q)$, i.e. we can assume that P is a p-group with cyclic Frattini subgroup and cyclic center. The automorphism groups of extraspecial p-groups have already been determined by Winter [32], so that we will not consider them in what follows.

Automorphisms of $X_{p^{2\ell+1}} * C_{p^{m+1}}$

Let p be an arbitrary prime and let $P = X_{p^{2\ell+1}} * C_{p^{m+1}}$ with $\ell \geq 1$ and $m \geq 1$. To begin, we fix some notation for the sequel. Let c be a generator of the cyclic group $Z(P) = C_{p^{m+1}}$ and let $z = c^{p^m}$. Let $x_1, y_1, \ldots, x_\ell, y_\ell$ be symplectic generators of the subgroup $X_{p^{2\ell+1}}$, all of order p and such that $[x_i, y_i] = z$.

Since $Z(P)$ is characteristic in P, restriction of automorphisms defines a homomorphism

$$\rho_{Z(P)} : \mathrm{Aut}(P) \to \mathrm{Aut}(Z(P)).$$

By definition, the kernel of $\rho_{Z(P)}$ is the subgroup $\mathrm{Aut}_{Z(P)}(P)$ of $\mathrm{Aut}(P)$.

Lemma 3.4.4. *The following extension of groups is split:*

$$1 \to \mathrm{Aut}_{Z(P)}(P) \to \mathrm{Aut}(P) \to \mathrm{Aut}(Z(P)) \to 1 \tag{3.1}$$

In particular, $\mathrm{Aut}(P) = \mathrm{Aut}_{Z(P)}(P) \rtimes \mathrm{Aut}(Z(P))$.

Proof. It is enough to show that there exists a homomorphic section, i.e. a homomorphism $\sigma : \mathrm{Aut}(Z(P)) \to \mathrm{Aut}(P)$ such that $\rho r = \mathrm{id}$. Since $Z(P)$ is cyclic, an automorphism $\alpha \in \mathrm{Aut}(Z(P))$ is defined by its value on the generator c of $Z(P)$. There exists thus an integer a prime to p such that $\alpha(c) = c^a$. The automorphism α is uniquely defined by the class of a modulo p^{m+1}.

We would like to extend α to an automorphism $\tilde{\alpha}$ of the whole group P. For this, we define $\tilde{\alpha}$ on the generators of P and check that the relations defining P are preserved. We set

$$\tilde{\alpha}(x_i) = x_i^a, \tag{3.2}$$

$$\tilde{\alpha}(y_i) = y_i, \tag{3.3}$$

$$\tilde{\alpha}(c) = \alpha(c) = c^a. \tag{3.4}$$

Let us check first that this definition does not depend on the choice of a representative of a modulo p^{m+1}. If $a \equiv a' \mod p^{m+1}$ then $x_i^a = x_i^{a'}$, since x_i has order p. Since c has order p^{m+1}, we also have $c^a = c^{a'}$.

The following sequence of equalities show that the relations $[x_i, y_i] = z$ are preserved by $\tilde{\alpha}$:

$$\tilde{\alpha}([x_i, y_i]) = [\tilde{\alpha}(x_i), \tilde{\alpha}(y_i)] = [x_i^a, y_i] = [x_i, y_i]^a = z^a = \tilde{\alpha}(z).$$

Similar and even easier calculations show that the other relations are also preserved. We can thus extend $\tilde{\alpha}$ to an endomorphism of P. Since a is prime to p, the map $\tilde{\alpha}$ is bijective, and hence $\tilde{\alpha} \in \mathrm{Aut}(P)$. It follows by definition that $\tilde{\alpha}$ extends α, so that we can define a section $\mathrm{Aut}(Z(P)) \to \mathrm{Aut}(P)$ by sending an automorphism α to $\tilde{\alpha}$. We still have to check that this section is a homomorphism.

Let $\alpha, \beta \in \mathrm{Aut}(Z(P))$, we have to check $\widetilde{\alpha\beta} = \tilde{\alpha}\tilde{\beta}$. It is enough to check this equality on the generators of P. This is trivially true on the generators y_i, $i = 1, \ldots, \ell$, since these maps are the identity on these elements. Let a be such that $\alpha(c) = c^a$ and let b be such that $\alpha(c) = c^b$. Since $\widetilde{\alpha\beta}$ does not depend on the representative of ab modulo p^{m+1}, we have

$$\widetilde{\alpha\beta}(x_i) = (x_i^{ab}) = (x_i^a)^b = (\tilde{\alpha}(x_i))^b = \tilde{\alpha}(x_i^b) = \tilde{\alpha}(\tilde{\beta}(x_i)).$$

A similar argument shows that $\widetilde{\alpha\beta}(c) = \tilde{\alpha}(\tilde{\beta}(c))$ and hence $\widetilde{\alpha\beta} = \tilde{\alpha}\tilde{\beta}$. We have then showed that the map $\alpha \mapsto \tilde{\alpha}$ is a homomorphic section and the lemma is proved. □

Remark 3.4.5.

a) In the previous proof, we could have equally well defined $\tilde{\alpha}$ as the identity on the x_i and $\tilde{\alpha}(y_i) = y_i^a$. We could also have chosen $\tilde{\alpha}(x_i) = x_i y_i$ and $\tilde{\alpha}(y_i) = y_i^a$. This should be enough to convince the reader that many more choices are possible and that the splitting is far from being unique.

b) Note that when $p = 2$, the elements x_i, y_i have order 2, so that α is extended as the identity on these elements.

The previous lemma allows us to identify $\mathrm{Aut}(Z(P))$ with a subgroup of $\mathrm{Aut}(P)$. From now on, we will often make no distinction between an automorphism of $Z(P)$ and its extension to P. If we need to make the identification precise, then we will use the notation $\tilde{\alpha}$ for the extension of α defined in the proof of Lemma 3.4.4.

Another characteristic subgroup of P is the Frattini subgroup $\Phi(P)$. We have then a homomorphism

$$\rho_{\Phi(P)} : \mathrm{Aut}(P) \to \mathrm{Aut}(\Phi(P)).$$

By definition the kernel of $\rho_{\Phi(P)}$ is the subgroup $\mathrm{Aut}_{\Phi(P)}(P)$ of $\mathrm{Aut}(P)$ and we will see below that $\rho_{\Phi(P)}$ does not split in general. Let us before recall briefly our notation for automorphisms of cyclic p-groups. We denote by θ the generator of the kernel of the restriction $\mathrm{Aut}(Z(P)) \to \mathrm{Aut}(\Phi(P))$. More precisely, θ is defined by $\theta(c) = c^{1+p^m} = cz$. When $p = 2$, we denote by τ the involution defined by $\tau(c) = c^{-1}$. Recall also that $\theta = \tau$ when $p = 2$ and $m = 1$.

Lemma 3.4.6. *Let $P = X_{p^{2\ell+1}} * C_{p^{m+1}}$ with $\ell \geq 1$ and $m \geq 1$.*

a) There is a commutative diagram with exact rows:

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Aut}_{Z(P)}(P) \arrow[r] \arrow[d] & \mathrm{Aut}(P) \arrow[r, "\rho_{Z(P)}"] \arrow[d, equal] & \mathrm{Aut}(Z(P)) \arrow[r] \arrow[d, "\rho^{Z(P)}_{\Phi(P)}"] & 1 \\
1 \arrow[r] & \mathrm{Aut}_{\Phi(P)}(P) \arrow[r] & \mathrm{Aut}(P) \arrow[r, "\rho_{\Phi(P)}"] & \mathrm{Aut}(\Phi(P)) \arrow[r] & 1
\end{tikzcd}$$

b) The first row splits and the second row splits if and only if either $m = 1$ or $p = 2$ and $m = 2$.

c) $\mathrm{Aut}_{\Phi(P)}(P) = \mathrm{Aut}_{Z(P)}(P) \rtimes \langle\theta\rangle$.

d) If either p is odd or $p = 2$ and $m > 1$, then $\mathrm{Aut}_{\Phi(P)}(P) = \langle\theta\rangle \times \mathrm{Aut}_{Z(P)}(P)$.

e) If p is odd and $m = 1$, then $\mathrm{Aut}(P) = \mathrm{Aut}_{\Phi(P)}(P) \rtimes \langle\beta\rangle$, where β is a generator of the cyclic group of order $p - 1$ of $\mathrm{Aut}(Z(P))$.

f) If $p = 2$ and $m = 1$, then $\mathrm{Aut}(P) = \mathrm{Aut}_{\Phi(P)}(P)$.

g) If $p = 2$ and $m = 2$, then $\mathrm{Aut}(P) = \mathrm{Aut}_{\Phi(P)}(P) \rtimes \langle\tau\rangle$.

Proof.

a) The fact that the first row is exact is the content of Lemma 3.4.4. Since $m > 1$, Lemma 3.2.5 gives that the vertical map $\rho^{Z(P)}_{\Phi(P)}$ is surjective. It follows that the map $\rho_{\Phi(P)}$ is surjective, so that the second row is exact.

b) It follows from Lemma 3.4.4 that the first row splits. Lemma 3.2.6 implies now that the second row splits if and only if the vertical map $\rho^{Z(P)}_{\Phi(P)}$ splits. We have seen in Lemma 3.2.5 that this maps splits if and only if either $m = 1$ or $p = 2$ and $m = 2$.

c) This follows from the splitting of $\rho_{Z(P)}$ and Lemma 3.2.6.

d) Let $\alpha \in \mathrm{Aut}_{Z(P)}(P)$, we check on the generators of P that $\theta\alpha\theta^{-1} = \alpha$. Since α is the identity on the characteristic subgroup $Z(P)$ of P, we have immediately that $(\theta\alpha\theta^{-1})(c) = c = \alpha(c)$. It remains to see that $(\theta\alpha\theta^{-1})(x_i) = \alpha(x_i)$ and $(\theta\alpha\theta^{-1})(y_i) = \alpha(y_i)$ for $i = 1, \dots, \ell$.

   Suppose first that p is odd. The subgroup $\Omega_1(P)$ of P is generated by the elements x_i, y_i, $i = 1, \dots, \ell$. Recall from Lemma 3.4.4 that the automorphism θ is extended to P as the identity on the y_i but also on the x_i, since $x_i^{1+p^m} = x_i$. It follows that θ is the identity on the characteristic subgroup $\Omega_1(P)$ of P. Therefore,
$$\theta\alpha\theta^{-1}(x_i) = \theta\alpha(x_i) = \alpha(x_i).$$
   We have similarly $(\theta\alpha\theta^{-1})(y_i) = \alpha(y_i)$ for all $i = 1, \dots, \ell$.

   Suppose now $p = 2$ and $m > 1$. The subgroup $\Omega_1(P)$ of P is generated by $w = c^{p^{m-1}}$ and the elements x_i, y_i, $i = 1, \dots, \ell$. Since $m > 1$, θ acts as the identity on w. The automorphism θ is extended to P as the identity on the elements x_i, y_i for $i = 1, \dots, \ell$. It follows that θ is the identity on the characteristic subgroup $\Omega_1(P)$ of P. Therefore, $(\theta\alpha\theta^{-1})(x_i) = \alpha(x_i)$ and $(\theta\alpha\theta^{-1})(y_i) = \alpha(y_i)$ for all $i = 1, \dots, \ell$.

e) Follows at once from the splitting of $\rho_{\Phi(P)}$ and the fact that $\mathrm{Aut}(\Phi(P))$ is cyclic of order $p - 1$.

f) If $p = 2$ and $m = 1$, the characteristic subgroup $\Phi(P)$ of P has order 2. It follows that $\Phi(P)$ is fixed pointwise by any automorphism of P, hence $\mathrm{Aut}_{\Phi(P)}(P) = \mathrm{Aut}(P)$.

g) Follows at once from the splitting of $\rho_{\Phi(P)}$.

□

Recall from Lemma 3.4.4 that $\mathrm{Aut}(P)$ is a semi-direct product $\mathrm{Aut}(P) = \mathrm{Aut}_{Z(P)}(P) \rtimes \mathrm{Aut}(Z(P))$. Since $Z(P)$ is cyclic, the structure of $\mathrm{Aut}(Z(P))$ is well known. Our next goal is to determine the structure of $\mathrm{Aut}_{Z(P)}(P)$. We denote π the homomorphism
$$\pi : \mathrm{Aut}_{Z(P)}(P) \to \mathrm{Aut}(P/Z(P))$$
obtained by the composition of the inclusion map $\mathrm{Aut}_{Z(P)}(P) \to \mathrm{Aut}(P)$ followed by the canonical homomorphism $\pi_{P/Z(P)} : \mathrm{Aut}(P) \to \mathrm{Aut}(P/Z(P))$. Recall that $V = P/Z(P)$ is a regular alternating space relatively to the form
$$b : V \times V \to P' \cong \mathbb{F}_p$$
induced by commutators. More precisely, for any $x, y \in P$ there exists $a \in \mathbb{Z}$ such that $[x, y] = z^a$ and $b(\overline{x}, \overline{y})$ is defined as the class of a modulo p. In order to simplify the notation, we will sometimes identify $b(\overline{x}, \overline{y})$ with $[x, y]$.

Since $P/Z(P)$ is a regular alternating space, we can consider the subgroup $Sp(P/Z(P))$ of $\mathrm{Aut}(P/Z(P)) = GL(P/Z(P))$ consisting of all linear transformations preserving b, namely
$$Sp(P/Z(P)) = \{\sigma \in \mathrm{Aut}(P/Z(P)) \,|\, b(\sigma(u), \sigma(v)) = b(u, v), \forall\, u, v \in P/Z(P)\}\,.$$

Since the alternating form is non-degenerate, we can choose a symplectic basis on $P/Z(P)$ in such a way that b is represented by the matrix

$$J = \begin{pmatrix} 0 & I_\ell \\ -I_\ell & 0 \end{pmatrix}$$

The group $Sp(P/Z/(P))$ can now be identified with the group $Sp(2\ell, p)$ of all matrices $A \in GL_{2\ell}(\mathbb{F}_p)$ such that $AJA^t = J$.

Lemma 3.4.7. *The image of* $\pi : \mathrm{Aut}_{Z(P)}(P) \to \mathrm{Aut}(P/Z(P))$ *is contained in* $Sp(P/Z(P))$.

Proof. Let $\alpha \in \mathrm{Aut}_{Z(P)}(P)$ and $\overline{x}, \overline{y} \in P/Z(P)$. We have to show that

$$b(\overline{\alpha}(\overline{x}), \overline{\alpha}(\overline{y})) = b(\overline{x}, \overline{y}). \tag{3.5}$$

By definition, the right-hand term is equal to $[x, y]$ and the left-hand term is equal to $[\alpha(x), \alpha(y)]$ as the following equalities show:

$$b(\overline{\alpha}(\overline{x}), \overline{\alpha}(\overline{y})) = b(\overline{\alpha(x)}, \overline{\alpha(y)}) = [\alpha(x), \alpha(y)].$$

Since P' is central and α restricts to the identity on P, we have $[\alpha(x), \alpha(y)] = [x, y]$ and the lemma is proved. $\square$

We have now an exact sequence

$$1 \to \ker \pi \to \mathrm{Aut}_{Z(P)}(P) \to S \to 1,$$

where $S = \mathrm{Im}\, \pi$ is a subgroup of $Sp(P/Z(P))$. Furthermore, we have by definition that $\ker \pi$ is equal to the group $\mathrm{Aut}_{Z(P),P/Z(P)}(P)$. The next lemma shows that this group is nothing more than the group $\mathrm{Int}(P)$ of inner automorphisms of P.

Lemma 3.4.8.

a) *The group* $\mathrm{Aut}_{Z(P),P/Z(P)}(P)$ *is equal to the group* $\mathrm{Int}(P)$ *and is elementary abelian of rank* 2ℓ.

b) *The automorphism* θ *commutes with any inner automorphism of* P *and*

$$\mathrm{Aut}_{\Phi(P),P/\Phi(P)}(P) = \mathrm{Int}(P) \times \langle \theta \rangle.$$

Proof.

a) It is clear that any inner automorphism of P restricts to the identity on $Z(P)$. Since P' is central, we have that $c_x(g) \in gZ(P)$ for any $x, g \in P$. We have thus that $\mathrm{Int}(P)$ is contained in $\mathrm{Aut}_{Z(P),P/Z(P)}(P)$. To prove the reverse inclusion, we simply show that these two groups have the same order.

   Recall first that there is a natural isomorphism $\mathrm{Int}(P) \cong P/Z(P)$, so that $\mathrm{Int}(P)$ is elementary abelian of rank 2ℓ. On the other hand, Lemma 3.2.1 implies that $\mathrm{Aut}_{Z(P),P/Z(P)}(P)$ is isomorphic to $\mathrm{Hom}(P/Z(P), Z(P))$. But $P/Z(P)$ is elementary abelian of rank 2ℓ and $Z(P)$ is cyclic of order p^{m+1}, hence $\mathrm{Hom}(P/Z(P), Z(P))$ is also elementary abelian of rank 2ℓ.

b) The automorphism θ is extended as the identity on the elements x_i and y_i for $i = 1, \ldots, \ell$, since $x_i^{1+p} = x_i$. We have therefore $\theta c_{x_i} \theta^{-1} = c_{\theta(x_i)} = c_{x_i}$ and the same equality holds with x_i replaced by y_i. This equality is trivially satisfied for z since c_z is the identity on P. It follows that θ commutes with all the generators of $\mathrm{Int}(P)$.

Since θ fixes $\Phi(P)$ but not $Z(P)$ pointwise, we have that $\theta \in \mathrm{Aut}_{\Phi(P)}(P)$ but $\theta \notin \mathrm{Int}(P)$. Hence $\mathrm{Int}(P) \times \langle\theta\rangle$ is elementary abelian of rank $2\ell + 1$ and is contained in $\mathrm{Aut}_{\Phi(P),P/\Phi(P)} \cong \mathrm{Hom}(P/\Phi(P), \Phi(P))$ which is elementary abelian of the same rank. It follows that these two groups are equal and the lemma is proved.

□

In Figure 3.1, the reader will find a drawing making some of the above results maybe a little bit more explicit.

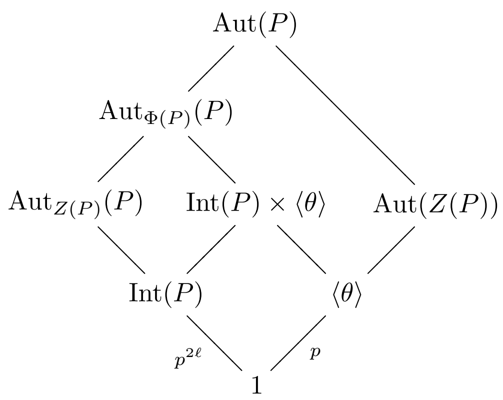

Figure 3.1: Structure of $\mathrm{Aut}(P)$ for $P = X_{p^{2\ell+1}} * C_{p^{m+1}}$.

Everything is now contained in the following proposition describing the automorphisms of $P = X_{p^{2\ell+1}} * C_{p^{m+1}}$.

Proposition 3.4.9. *Let $P = X_{p^{2\ell+1}} * C_{p^{m+1}}$ with $\ell \geq 1$ and $m \geq 1$. Then*

$$\mathrm{Aut}(P) = \mathrm{Aut}_{Z(P)}(P) \rtimes \mathrm{Aut}(Z(P))$$

and there is an exact sequence

$$1 \to \mathrm{Int}(P) \to \mathrm{Aut}_{Z(P)}(P) \to Sp(2\ell, p) \to 1.$$

Proof. A great part of the job has already been done. The decomposition $\mathrm{Aut}(P) = \mathrm{Aut}_{Z(P)}(P) \rtimes \mathrm{Aut}(Z(P))$ is the content of Lemma 3.4.4. The kernel of π is $\mathrm{Aut}_{Z(P),P/Z(P)}(P)$ and we have seen in Lemma 3.4.8 that this group is equal to the group $\mathrm{Int}(P)$. The preceding lemma shows that $\mathrm{Im}\,\pi$ is contained in $Sp(P/Z(P)) \cong Sp(2\ell, p)$, so that it only remains to show that π is surjective on $Sp(P/Z(P))$.

To begin, we reorder the elements $x_1, y_1, \ldots, x_\ell, y_\ell$. For $j = 1, \ldots, \ell$ we let $w_j = x_j$ and $w_{j+\ell} = y_j$. We have in this way

$$[w_i, w_j] = \begin{cases} z & \text{if } |i - j| = \ell. \\ 1 & \text{else.} \end{cases}$$

Let $\mathcal{B} = \{\overline{w}_1, \ldots, \overline{w}_{2\ell}\}$ be the basis of $P/Z(P)$ where $\overline{w}_i$ is the class of w_i in $P/Z(P)$. Relatively to this basis, the alternating form b is represented by the matrix

$$\begin{pmatrix} 0 & I_\ell \\ -I_\ell & 0 \end{pmatrix}.$$

Let σ be an automorphism of $P/Z(P)$ which preserves the alternating form b. With respect to the basis $\mathcal{B}$ the automorphism σ is represented by a matrix $s = (s_{l,k}) \in Sp(2\ell, p)$. Precisely,

$$\sigma(\overline{w}_i) = \overline{w}_1^{s_{1,i}} \overline{w}_2^{s_{2,i}} \cdots \overline{w}_{2\ell}^{s_{2\ell,i}}.$$

We define $\tilde{\sigma} : P \to P$ on the generators P by

$$\tilde{\sigma}(w_i) = w_1^{s_{1,i}} w_2^{s_{2,i}} \cdots w_{2n}^{s_{2n,i}} \text{ and } \tilde{\sigma}(c) = c.$$

Clearly, with this definition, $\overline{\tilde{\sigma}(w_i)} = \sigma(\overline{w}_i)$, and since σ preserves the symplectic form b, we have

$$[\tilde{\sigma}(w_i), \tilde{\sigma}(w_j)] = b(\overline{\tilde{\sigma}(w_i)}, \overline{\tilde{\sigma}(w_j)}) = b(\sigma(\overline{w}_i), \sigma(\overline{w}_j)) = b(\overline{w}_i, \overline{w}_j) = [w_i, w_j].$$

Furthermore, if p is odd,

$$\tilde{\sigma}(w_i)^p = \left(w_1^{s_{1,i}} \cdots w_{2\ell}^{s_{2\ell,i}}\right)^p = (w_1^{s_{1,i}})^p \cdots (w_{2\ell}^{s_{2\ell,i}})^p = 1.$$

Since σ is an automorphism we have $\tilde{\sigma}(w_i) \neq 1$, hence $\tilde{\sigma}(w_i)$ has order p.

For $p = 2$ we have that $\tilde{\sigma}(w_i)^2$ is in P'. If $\tilde{\sigma}(w_i)^2 \neq 1$, we modify $\tilde{\sigma}(w_i)$ by letting

$$\tilde{\sigma}(w_i) = c^{2^{m-1}} \cdot (w_1^{s_{1,i}} w_2^{s_{2,i}} \cdots w_{2n}^{s_{2n,i}}).$$

instead of the previous definition of $\tilde{\sigma}(w_i)$. In this way we have $\tilde{\sigma}(w_i)^2 = 1$ for all $i = 1, \ldots, 2\ell$. Since $u^{2^{m-1}}$ is in $Z(P)$ this does not affect the commuting relations, so that $\tilde{\sigma}$ preserves all the relations defining P.

This shows that $\tilde{\sigma}$ extends to an endomorphism of P. As σ is an automorphism, $\overline{w}_i = \sigma(\overline{v}_i)$ for some $v_i \in P$. Therefore

$$\overline{w}_i = \sigma(\overline{v}_i) = \overline{\tilde{\sigma}(v_i)},$$

so that $w_i = \tilde{\sigma}(v_i)h$ for some $h \in Z(P)$. But then $w_i = \tilde{\sigma}(v_i)\tilde{\sigma}(h) = \tilde{\sigma}(v_i h)$, since $\tilde{\sigma}$ acts trivially on $Z(P)$. It follows that w_i is in the image of $\tilde{\sigma}$, proving that $\tilde{\sigma}$ is an automorphism of P. □

Remark 3.4.10. The condition $m \geq 1$ is really necessary only if $p = 2$. When p is odd, all our above results still hold under the assumption $m = 0$. In this situation, P is extraspecial of exponent p and we recover the results of Winter [32]. If $p = 2$ and $m = 0$, then $P = D_8^{*\ell}$ and in this situation there is a quadratic form $q : P/Z(P) \to \Phi(P)$ given by $q(\overline{x}) = x^2$ and one obtains in this case a similar result to the above proposition, but with the symplectic group $Sp(2\ell, p)$ replaced by the orthogonal group $O^+(2\ell, p)$. The details can be found in Winter's paper [32].

We will see below under which conditions the extension

$$1 \to \mathrm{Int}(P) \to \mathrm{Aut}_{Z(P)}(P) \to Sp(2\ell, p) \to 1$$

is split. We give before two immediate corollaries of the preceding proposition.

Corollary 3.4.11. *Let $P = X_{p^{2\ell+1}} * C_{p^{m+1}}$ with $\ell \geq 1$ and $m \geq 1$. Then*

$$\mathrm{Out}(P) \cong Sp(2\ell, p) \rtimes \mathrm{Aut}(C_{p^{m+1}}).$$

Corollary 3.4.12. *Let $P = X_{p^{2\ell+1}} * C_{p^{m+1}}$ with $\ell \geq 1$ and $m \geq 1$. Then*

$$|\mathrm{Aut}(P)| = p^{(\ell+1)^2+m-1}(p-1)\prod_{i=1}^{\ell}(p^{2i}-1).$$

Proposition 3.4.13. *Let $P = X_{p^{2\ell+1}} * C_{p^{m+1}}$ with $\ell \geq 1$ and $m \geq 1$. Let*

$$1 \to \mathrm{Int}(P) \to \mathrm{Aut}_{Z(P)}(P) \to Sp(2\ell, p) \to 1. \tag{3.6}$$

be the extension of groups obtained in Proposition 3.4.9. Then

a) If p is odd, the extension (3.6) is split.

b) If $p = 2$ and $\ell \geq 3$, the extension (3.6) is not split.

Proof. In the case p odd, there is a standard argument due to Griess and Isaacs (see [16, Chapter 7]). This argument goes as follows.

Let J be the preimage of the central involution $-Id$ under the map $\pi : \mathrm{Aut}_{Z(P)}(P) \to Sp(2\ell, p)$. Since p is odd, $N = \pi^{-1}(\langle -Id\rangle) = \mathrm{Int}(P) \rtimes \langle J\rangle$ and J acts on $\mathrm{Int}(P)$ by sending each element to its inverse. Furthermore, N is normal in $\mathrm{Aut}_{Z(P)}(P)$ (since $\langle -Id\rangle$ is normal in $Sp(2\ell, p)$) and $\langle J\rangle$ is a 2-Sylow subgroup of N since p is odd and $\mathrm{Int}(P) \cong (C_p)^{2\ell}$. It follows by the Frattini argument that $\mathrm{Aut}_{Z(P)}(P)$ is generated by $N_{\mathrm{Aut}_{Z(P)}(P)}(\langle J\rangle)$ and N. But since J has order 2, $N_{\mathrm{Aut}_{Z(P)}(P)}(\langle J\rangle) = C_{\mathrm{Aut}_{Z(P)}(P)}(\langle J\rangle)$ and J is not centralized by any element of $\mathrm{Int}(P)$. It follows that $N_{\mathrm{Aut}_{Z(P)}(P)}(\langle J\rangle) \cap \mathrm{Int}(P) = \{1\}$, so that $N_{\mathrm{Aut}_{Z(P)}(P)}(\langle J\rangle)$ is a complement to $\mathrm{Int}(P)$ in $\mathrm{Aut}_{Z(P)}(P)$.

Suppose now $p = 2$ and $\ell \geq 3$. Griess proved in [15, Corollary 2] that the extension (3.6) is not split when $m = 1$, i.e. when $P = D_8^{*\ell} * C_4$. Suppose now $m > 1$, and let D be the subgroup of P generated by w and the x_i, y_i, $1 \leq i \leq \ell$, so that $D = D_8^{*\ell} * C_4$. Any automorphism of D fixing $Z(D) = \langle w\rangle$ pointwise can be extended to an automorphism of P by letting it act trivially on $Z(P)$. This defines an injective homomorphism

$$\mathrm{Aut}_{Z(D)}(D) \hookrightarrow \mathrm{Aut}_{Z(P)}(P).$$

The inner automorphisms of D are then sent to inner automorphisms of P and we have the following commutative diagram

$$\begin{tikzcd} 1 \arrow[r] & \mathrm{Int}(P) \arrow[r] & \mathrm{Aut}_{Z(P)}(P) \arrow[r] & Sp(2\ell,2) \arrow[r] & 1 \\ 1 \arrow[r] & \mathrm{Int}(D) \arrow[r] \arrow[u] & \mathrm{Aut}_{Z(D)}(D) \arrow[r] \arrow[u] & Sp(2\ell,2) \arrow[r] \arrow[u, equal] & 1 \end{tikzcd}$$

The first row does not split since the second one does not by Griess' result [15, Corollary 2]. □

Remark 3.4.14. We don't know whether the extension splits or not, when $p = 2$ and $\ell \in \{1, 2\}$.

We end up this part on automorphisms of $P = X_{p^{2\ell+1}} * C_{p^{m+1}}$ with a last remark on the special case $p = 2$ and $m = 1$. In this situation, $P = D_8^{*\ell} * C_4$ and $P/\Phi(P)$ is endowed with a quadratic form

$$q : P/\Phi(P) \to \Phi(P) \cong \mathbb{F}_2$$

given by $q(\overline{x}) = x^2$. Since $\Phi(P)$ has order 2, any automorphism α of P restricts to the identity on $\Phi(P)$. Furthermore, if $\overline{\alpha}$ is the automorphism induced by α on $P/\Phi(P)$, then

$$q(\overline{\alpha}(\overline{x})) = q(\overline{\alpha(x)}) = (\alpha(x))^2 = \alpha(x^2) = x^2 = q(\overline{x}).$$

Therefore, $\overline{\alpha}$ preserves the quadratic form q and there is thus a well-defined homomorphism

$$\pi : \mathrm{Aut}(P) \to O(P/\Phi(P), q) = O(2\ell + 1, 2).$$

The kernel of π is easily seen to be generated by $\mathrm{Int}(P)$ and the extension to P of the automorphism $\theta \in \mathrm{Aut}(Z(P))$ sending $c \to cz = c^{1+2}$, where c is the generator of $Z(P)$. We have seen furthermore in Lemma 3.4.6 that when $P = D_8^{*\ell} * C_4$, then $\mathrm{Aut}(P) = \mathrm{Aut}_{Z(P)}(P) \rtimes \langle\theta\rangle$. All this shows that there is an exact sequence

$$1 \to \mathrm{Int}(P) \to \mathrm{Aut}_{Z(P)}(P) \to O(2\ell + 1, 2) \to 1$$

We recover then the result of Proposition 3.4.9 thanks to the isomorphism between $O(2\ell + 1, 2)$ and $Sp(2\ell, 2)$.

Automorphisms of $X_{p^{2\ell+1}} * M_{p^{m+2}}$

Let $P = X_{p^{2\ell+1}} * M_{p^{m+2}}$ with $\ell \geq 0$ and $m > 1$. We fix notation for the sequel. Let a, u be generators of the subgroup $M_{p^{m+2}}$ with a of order p, u of order p^{m+1} and $aua^{-1} = u^{1+p^m}$. Let $z = u^{p^m}$ and let $x_1, y_1, \ldots, x_\ell, y_\ell$ be symplectic generators of the subgroup $X_{p^{2\ell+1}}$ all of order p and such that $[x_i, y_i] = z$.

In this situation, we have that $Z(P) = \Phi(P)$ is maximal in the subgroup $U = \langle u\rangle$ and we denote by $c = u^p$ the generator of $Z(P)$.

The first main difference with the previous case is that, in general, the group $\mathrm{Aut}(P)$ is not a semi-direct product $\mathrm{Aut}_{Z(P)}(P) \rtimes \mathrm{Aut}(Z(P))$ anymore as the next lemma shows. The reason is roughly that $Z(P)$ is not a maximal cyclic subgroup of P anymore. We will see in Lemma 3.4.16 that the automorphisms of U, which is maximal cyclic in P, can be extended homomorphically to P.

Lemma 3.4.15. *The following sequence is exact*

$$1 \to \mathrm{Aut}_{Z(P)}(P) \to \mathrm{Aut}(P) \to \mathrm{Aut}(Z(P)) \to 1$$

and splits if and only if $p = 2$ and either $m = 2$ or $m = 3$.

Proof. To show the exactness of the sequence, it is enough to show that an automorphism of $Z(P)$ can be extended to P. If $\alpha \in \mathrm{Aut}(Z(P))$ then $\alpha(c) = c^k$ with k prime to p and uniquely defined modulo p^m. We extend α by letting

$$\begin{aligned}\tilde{\alpha}(x_i) &= x_i^k,\\ \tilde{\alpha}(y_i) &= y_i,\\ \tilde{\alpha}(a) &= a,\\ \tilde{\alpha}(u) &= u^k.\end{aligned}$$

As defined, $\tilde{\alpha}$ preserves all the relations and defines an automorphism of P that extends α (see 3.4.4 for details). Note that this definition depends on the chosen representative of k modulo p^m since u has order p^{m+1}. We show now the assertion on the splitting of the sequence. Suppose that σ is a homomorphic section. Suppose first that p is odd and let $\alpha \in \mathrm{Aut}(Z(P))$ be the automorphism of $Z(P)$ defined by $\alpha(c) = c^{1+p}$. Note that this automorphism has order p^{m-1}. The automorphism $\sigma\alpha$ sends u to $u^h x$, for some $h \not\equiv 0 \mod p$, and some x in the subgroup generated by the x_i, y_i and a, that is, $x \in \Omega_1(P)$. In particular, $x^p = 1$ and we have

$$c^{1+p} = \alpha(c) = (\sigma\alpha)(c) = (\sigma\alpha)(u^p) = (u^h x)^p = u^{ph} x^p = u^{ph} = c^h.$$

It follows that $h \equiv 1 + p \mod p^m$, i.e. $h = 1 + p + tp^m$. We have therefore

$$(\sigma\alpha)(u) = u^{1+p} z^t x.$$

The element x can be written as $x'a^\varepsilon$ with $x' \in \langle x_i, y_i, i = 1, \dots, \ell\rangle$ and $0 \le \varepsilon \le p - 1$.

If $x' = 1$, i.e. $x = a^\varepsilon$, we choose γ to be the automorphism of P defined by $\gamma(u) = ua^\varepsilon$ and the identity on all the other generators. If $x' \neq 1$ then without loss of generality we may assume $x' = x_1$. In this situation, we choose γ to be the automorphism of P defined by $\gamma(u) = ux$, $\gamma(a) = a$, $\gamma(x_1) = x_1$, $\gamma(y_1) = y_1 a$ and γ is the identity on the other generators, namely x_j, y_j for $j \neq 1$. In both cases γ has order p.

Let β be the automorphism of P defined by $\beta(u) = u^{1+p}$ and the identity on the other generators. By our definitions, we have $(\sigma\alpha)(u) = \beta\gamma(u)$. Since $m > 1$, we have $\beta\gamma \neq 1$ and $(\beta\gamma)^p = \beta^p$, so that $\beta\gamma$ has order p^m. It follows that $\sigma\alpha$ has order p^m and this contradicts the fact that σ is a homomorphism.

Suppose now $p = 2$ and $m = 2$. Then $\mathrm{Aut}(Z(P))$ is cyclic of order 2 generated by the involution δ sending c to c^{-1}. We define $\tilde{\delta}$ as the automorphism of P given by $\tilde{\delta}(u) = u^{-1}$ and the identity on all other generators. Note that this is a well-defined automorphism of P since P' has order 2 and thus $[a, u^{-1}] = [a, u]$ so that all relations will be preserved. The map $\mathrm{Aut}(Z(P)) \to \mathrm{Aut}(P)$ given by $\delta \mapsto \tilde{\delta}$ is the desired homomorphic section.

Suppose now $p = 2$ and $m = 3$. The group $\mathrm{Aut}(Z(P))$ is elementary abelian of rank 2 generated by $u^2 \mapsto (u^2)^5 = u^2 z$ and the involution $u^2 \mapsto (u^2)^{-1}$.

Consider the automorphism δ of P given by $\delta(u) = ux_1y_1$, $\delta(a) = a$, $\delta(x_1) = x_1a$, $\delta(y_1) = y_1a$ and δ is the identity on the remaining generators, namely the x_j, y_j for $j \neq 1$. As defined δ is an automorphism of order 2 and

$$\delta(u^2) = u^2 z = u^2(u^2)^4 = u^5.$$

We have thus a homomorphic section of $\rho_{Z(P)}$. The case $p = 2$ and $m \geq 4$ can be dealt similarly to the case p odd. □

Lemma 3.4.16. *There is an injective homomorphism*

$$\mathrm{Aut}(U) \hookrightarrow \mathrm{Aut}(P)$$

Proof. If α is an automorphism of U, then $\alpha(u) = u^k$ for some k prime to p. Furthermore, k is unique modulo p^{m+1}. We can define $\tilde{\alpha}$ on the generators of P by letting

$$\tilde{\alpha}(x_i) = x_i^k,$$
$$\tilde{\alpha}(y_i) = y_i,$$
$$\tilde{\alpha}(a) = a,$$
$$\tilde{\alpha}(u) = \alpha(u) = u^k.$$

We have to check that the relations defining P are preserved. Since k is prime to p, it is immediate that the order of the generators are preserved. For the relations $[x_i, y_i] = z$, $(1 \leq i \leq \ell)$, we obtain

$$\tilde{\alpha}([x_i, y_i]) = [\tilde{\alpha}(x_i), \tilde{\alpha}(y_i)] = [x_i^k, y_i] = [x_i, y_i]^k = z^k = \alpha(z) = \tilde{\alpha}(z).$$

Similarly, for the relation $[a, u] = z$ we obtain

$$\tilde{\alpha}([a, u]) = [a, u^k] = z^k = \tilde{\alpha}(z).$$

The remaining relations are verified with a similar argument and this shows that $\tilde{\alpha}$ extends to an endomorphism of P. Since k is prime to p, $\tilde{\alpha}$ is easily seen to be an automorphism of P. This shows that any automorphism α of U can be extended to an automorphism $\tilde{\alpha}$ of P. We still have to show that the map sending α to $\tilde{\alpha}$ is a homomorphism.

Let $\alpha, \beta \in \mathrm{Aut}(Z(P))$, we have to check that $\widetilde{\alpha\beta} = \tilde{\alpha}\tilde{\beta}$. It is enough check this equality on the generators of P. This is trivially true on the y_i, $i = 1, \ldots, \ell$, since these maps are the identity on these elements. Let r be such that $\alpha(u) = u^s$ and let r be such that $\beta(u) = u^s$. Since $\widetilde{\alpha\beta}$ does not depend on the chosen representative of ab modulo p^{m+1}, we have then $\alpha\beta(u) = u^{rs}$ so that

$$\widetilde{\alpha\beta}(x_i) = (x_i^{rs}) = (x_i^r)^s = (\tilde{\alpha}(x_i))^s = \tilde{\alpha}(x_i^s) = \tilde{\alpha}(\tilde{\beta}(x_i)).$$

A similar argument shows that $\widetilde{\alpha\beta}(u) = \tilde{\alpha}(\tilde{\beta}(u))$ and hence $\widetilde{\alpha\beta} = \tilde{\alpha}\tilde{\beta}$. We have then showed that the map $\mathrm{Aut}(U) \to \mathrm{Aut}(P)$ given by $\alpha \mapsto \tilde{\alpha}$ is a homomorphism. If $\tilde{\alpha}$ is the identity on P, then it is also the identity on the subgroup U and therefore α is the identity. This shows that this homomorphism $\mathrm{Aut}(U) \to \mathrm{Aut}(P)$ is injective and the lemma is proved. □

From now on, we identify $\mathrm{Aut}(U)$ with its image in $\mathrm{Aut}(P)$. With this identification, we have the following two results.

Lemma 3.4.17. *Let $\theta \in \mathrm{Aut}(U)$ be the automorphism of U defined by $\theta(u) = u^{1+p^m} = uz$. Then*

$$\mathrm{Aut}(U) \cap \mathrm{Aut}_{Z(P)}(P) = \langle \theta \rangle.$$

Proof. As a subgroup of $\mathrm{Aut}(U)$, the intersection $\mathrm{Aut}(U) \cap \mathrm{Aut}_{Z(P)}(P)$ is the kernel of the restriction map $\rho^U_{Z(P)} : \mathrm{Aut}(U) \to \mathrm{Aut}(Z(P))$. Since $m > 1$, Lemma 3.2.5 gives that $\ker \rho^U_{Z(P)}$ is generated by θ and the lemma is proved. □

Lemma 3.4.18. *The subgroup $\mathrm{Aut}_U(P)$ is not normal in $\mathrm{Aut}(P)$.*

Proof. Since $m > 1$ the element ua has the same order as u and we let α be the automorphism of P defined as $\alpha(u) = ua$ and as the identity on the other generators of P. The inner automorphism c_u is in $\mathrm{Aut}_U(P)$ and we have

$$\alpha c_u \alpha^{-1}(u) = \alpha c_u(ua^{-1}) = \alpha(u(az)^{-1}) = uaa^{-1}z^{-1} = uz^{-1}.$$

Therefore $\alpha c_u \alpha^{-1} \notin \mathrm{Aut}_U(P)$, so that $\mathrm{Aut}_U(P)$ is not normal in $\mathrm{Aut}(P)$. □

Remark 3.4.19. We have seen above two different ways to decompose $\mathrm{Aut}(P)$. The first one is to see $\mathrm{Aut}(P)$ as generated by the two subgroups $\mathrm{Aut}(U)$ and $\mathrm{Aut}_U(P)$. This has the advantage of giving a decomposition of P as a product of two subgroups with a trivial intersection. However, none of these two subgroups is canonical, since both are not normal in $\mathrm{Aut}(P)$. The second way of decomposing $\mathrm{Aut}(P)$ is as the product of the two subgroups $\mathrm{Aut}(U)$ and $\mathrm{Aut}_{Z(P)}(P)$. But now, one of the two subgroups, namely $\mathrm{Aut}_{Z(P)}(P)$ is normal in $\mathrm{Aut}(P)$. For this reason, we will prefer this decomposition even though the intersection is not trivial. However, this intersection is reasonably small since it is has order p by Lemma 3.4.17.

We make next some observations on the inner automorphisms of P.

Lemma 3.4.20. *Let $\theta \in \mathrm{Aut}(U)$ be defined by $\theta(u) = u^{1+p^m} = uz$.*

a) $\theta = c_a$.

b) $\mathrm{Int}(P) = \mathrm{Int}_U(P) \times \langle \theta \rangle$ is elementary abelian of rank $2\ell + 2$.

c) $\mathrm{Int}_U(P)$ is elementary abelian of rank $2\ell + 1$.

Proof.

a) By definition $c_a(u) = uz$ and c_a is the identity on the remaining generators of P. It follows immediately that $\theta = c_a$.

b) The group $\mathrm{Int}(P)$ is elementary abelian of rank $2(\ell + 1)$ and has a basis given by the inner automorphisms $\{c_u, c_a, c_{x_i}, c_{y_i}, i = 1, \dots, \ell\}$. The only basis element that acts non-trivially on $U = \langle u \rangle$ is $c_a = \theta$. It follows that

$$\mathrm{Int}(P) = \langle c_u, c_{x_i}, c_{y_i}, i = 1, \dots, \ell \rangle \times \langle c_a \rangle = \mathrm{Int}_U(P) \times \langle \theta \rangle.$$

c) Follows immediately from part b) and the fact that $\mathrm{Int}(P) \cong P/Z(P)$ is elementary abelian of rank $2(\ell+1)$ and θ has order p.

□

The reader will find in Figure 3.2 a more visual description of some of the above results.

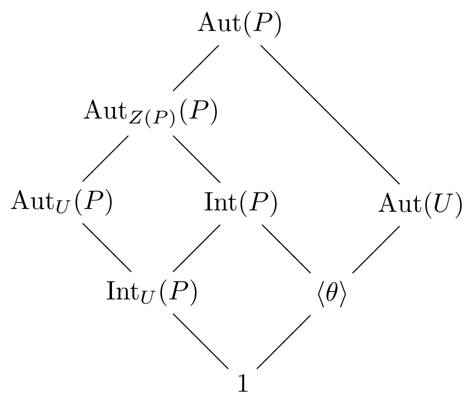

Figure 3.2: Structure of $\mathrm{Aut}(P)$ for $P = X_{p^{2\ell+1}} * M_{p^{m+2}}$.

We turn now our attention to the subgroup $\mathrm{Aut}_{Z(P)}(P)$ of $\mathrm{Aut}(P)$. Recall that $V = P/Z(P)$ is a regular alternating space relatively to the map

$$b : V \times V \to \mathbb{F}_p$$

induced by commutators. In particular, we denote by $Sp(V)$ or $Sp(P/Z(P))$ the subgroup of all automorphisms of $P/Z(P)$ preserving the alternating form b. Recall also that there is a linear map

$$\varphi : V \to Z(P)/\Omega^1(Z(P)) \cong \mathbb{F}_p$$

induced by taking p-th powers.

Definition 3.4.21. Let b be a non-degenerate alternating form on a vector space V over a field $\mathbb{F}$ and let $\varphi : V \to F_p$ be a non-zero linear form on V. We define $Sp_\varphi(V)$ as the subgroup of $GL(V)$ consisting of all linear transformations preserving b and φ, namely

$$Sp_\varphi(V) = \{\sigma \in GL(V) \,|\, b(\sigma v, \sigma w) = b(v, w) \text{ and } \varphi(\sigma v) = \varphi(v), \, \forall v, w \in V\}\,.$$

The structure of the group $Sp_\varphi(V)$ has already been reasonably well described by Winter in [32] where this group appears in the study of the automorphism group of odd order extraspecial p-groups of exponent p^2. The proof of the following lemma can be found along the lines of Winter's paper.

Lemma 3.4.22. *Let p be a prime and let V be vector space of over $\mathbb{F}_p$. Let $b : V \times V \to \mathbb{F}_p$ be a non-degenerate alternating form on V and let $\varphi : V \to \mathbb{F}_p$ be a non-zero linear form on V. Then $Sp_\varphi(V)$ is the semi-direct product of $Sp(2(n-1), p)$ acting on an extraspecial p-group of type I and exponent p.*

More precisely, let $\mathcal{B} = \{e_1, f_1, \ldots, e_n, f_n\}$ be a symplectic basis of V such that $\varphi(e_j) = \varphi(f_j) = 0 = \varphi(e_n)$ for $1 \leq j \leq n-1$ and $\varphi(f_n) = 1$. Let S be the subgroup of $Sp(2n, p)$ consisting of matrices of the form

$$\left(\begin{array}{c|c} A' & 0 \\ \hline 0 & I_2 \end{array}\right)$$

with $A' \in Sp(2(n-1), p)$. Let N be the subgroup of $Sp(2n, p)$ consisting of matrices of the form

$$\left(\begin{array}{ccccc|cc} & & & & & 0 & -v_1 \\ & & & & & 0 & u_1 \\ & & I_{2(n-1)} & & & \vdots & \vdots \\ & & & & & 0 & -v_{n-1} \\ & & & & & 0 & u_{n-1} \\ \hline u_1 & v_1 & \cdots & u_{n-1} & v_{n-1} & 1 & z \\ 0 & 0 & \cdots & 0 & 0 & 0 & 1 \end{array}\right)$$

Then $S \cong Sp(2(n-1), p)$, N is extraspecial of type I and order $2^{2(n-1)+1}$ and $Sp_\varphi(V)$ is isomorphic to the semi-direct product of S acting on N.

Proof. A detailed proof can be found in [32]. We will however give an idea on how the proof goes. Let $\alpha \in Sp_\varphi(V)$ and let A be the matrix of α relatively to the basis $\mathcal{B}$. The kernel of φ has basis $\{e_j, f_j, e_n, j = 1, \ldots, n-1\}$ and $\langle e_n \rangle = (\ker \varphi)^\perp$. Since α preserves φ and b, we have that α stabilizes $\ker \varphi$ and $(\ker \varphi)^\perp$. For the same reason, $\alpha(f_n) = f_n + w$ with $w \in \ker \varphi$. It follows then that $\alpha(e_n) = \lambda e_n$ for some $\lambda \in \mathbb{F}_p$ and then

$$1 = b(e_n, f_n) = b(\alpha e_n, \alpha f_n) = b(\lambda e_n, f_n + w) = \lambda b(e_n, f_n) = \lambda.$$

Therefore $\alpha(e_n) = e_n$ and we have that the matrix A of α relatively to $\mathcal{B}$ has the following form

$$\left(\begin{array}{ccc|cc} & & & 0 & * \\ & A' & & \vdots & \vdots \\ & & & 0 & * \\ \hline * & \cdots & * & 1 & * \\ 0 & \cdots & 0 & 0 & 1 \end{array}\right)$$

Furthermore, A' is the matrix of the homomorphism induced by α on the non-degenerate vector space $V/\langle e_n, f_n \rangle$, so that $A' \in Sp(2(n-1), p)$. $\square$

We denote by

$$\pi : \mathrm{Aut}_{Z(P)}(P) \to \mathrm{Aut}(P/Z(P))$$

the composition of the inclusion map $\mathrm{Aut}_{Z(P)}(P) \to \mathrm{Aut}(P)$ followed by the canonical map $\pi_{P/Z(P)} : \mathrm{Aut}(P) \to \mathrm{Aut}(P/Z(P))$.

Lemma 3.4.23. *The image of the map $\pi : \mathrm{Aut}_{Z(P)}(P) \to \mathrm{Aut}(P/Z(P))$ is contained in $Sp_\varphi(P/Z(P))$.*

Proof. Let $\alpha \in \mathrm{Aut}_{Z(P)}(P)$. By definition, we have

$$b(\overline{\alpha}(\overline{x}), \overline{\alpha}(\overline{y})) = b(\overline{\alpha(x)}, \overline{\alpha(y)}) = [\alpha(x), \alpha(y)] = \alpha([x, y]) = [x, y] = b(\overline{x}, \overline{y}).$$

The equality $\alpha([x, y]) = [x, y]$ follows from our choice of α in $\mathrm{Aut}_{Z(P)}(P)$ and the fact that P' is central. This shows that $\mathrm{Im}\,\pi$ is contained in $Sp(P/Z(P))$. For the same reason we have the following equalities

$$\varphi(\overline{\alpha}(\overline{x})) = \varphi(\overline{\alpha(x)}) = (\alpha(x))^p = \alpha(x^p) = x^p = \varphi(\overline{x}).$$

This shows that $\mathrm{Im}\,\pi$ is contained in $Sp_\varphi(P/Z(P))$ and the lemma is proved. $\square$

Lemma 3.4.24. *The kernel of π is equal to the group $\mathrm{Int}(P)$.*

Proof. The kernel of π is equal to the group $\mathrm{Aut}_{Z(P),P/Z(P)}(P)$ which is isomorphic to $\mathrm{Hom}(P/Z(P), Z(P))$ by Lemma 3.2.1. Since $P/Z(P)$ is elementary abelian and $Z(P)$ is cyclic, we have that $\mathrm{Hom}(P/Z(P), Z(P))$ has order $p^{2\ell+2}$.

Since $P' \le Z(P)$, we have that $\mathrm{Int}(P)$ is contained in $\mathrm{Aut}_{Z(P),P/Z(P)}(P)$, but these groups have the same order since $P/Z(P)$ is elementary abelian of rank $2\ell + 2$. Therefore $\mathrm{Int}(P) = \mathrm{Aut}_{Z(P),P/Z(P)}(P) = \ker \pi$. $\square$

Proposition 3.4.25. *Let $P = X_{p^{2\ell+1}} * M_{p^{m+2}}$ with $\ell \ge 0$ and $m > 1$. Then*

a) $\mathrm{Aut}(P)$ *is generated by* $\mathrm{Aut}_{Z(P)}(P)$ *and a subgroup $H \cong \mathrm{Aut}(C_{p^{m+1}})$ with* $\mathrm{Aut}_{Z(P)}(P) \cap H$ *cyclic of order p.*

b) There is an exact sequence

$$1 \to \mathrm{Int}(P) \to \mathrm{Aut}_{Z(P)}(P) \to Sp_\varphi(P/Z(P)) \to 1.$$

Furthermore, $\mathrm{Int}(P)$ *is isomorphic to $C_p^{2(\ell+1)}$ and $Sp_\varphi(P/Z(P))$ is isomorphic to a semi-direct product of $Sp(2\ell, p)$ acting on an extraspecial p-group of type I and order $p^{2\ell+1}$.*

Proof. a) Recall from Lemma 3.4.16 that $\mathrm{Aut}(U)$ can be identified with a subgroup H of $\mathrm{Aut}(P)$. More precisely, if $\alpha(u) = u^k$, then α is extended by $\alpha(x_i) = x_i^k$ and as the identity on the other generators. If α is in the intersection $H \cap \mathrm{Aut}_{Z(P)}(P)$, then α is the kernel of the restriction homomorphism $\mathrm{Aut}(U) \to \mathrm{Aut}(Z(P))$, hence is contained in $\langle\theta\rangle$, where θ is defined by $\theta(u) = u^{1+p^m}$. We have of course $\theta \in \mathrm{Aut}_{Z(P)}(P)$, so that $H \cap \mathrm{Aut}_{Z(P)}(P) = \langle\theta\rangle$ and has order p. This proves our first assertion.

b) We know from Lemma 3.4.23 that the image of the homomorphism $\pi : \mathrm{Aut}_{Z(P)}(P) \to \mathrm{Aut}(P/Z(P))$ is contained in the subgroup $Sp_\varphi(P/Z(P))$ and we know from Lemma 3.4.24 that $\ker \pi = \mathrm{Int}(P)$. It remains thus to see that π is surjective on $Sp_\varphi(P/Z(P))$.

To begin, we reorder the generators of P in the following way. We let

$$w_j = \begin{cases} x_j & \text{if } j = 1, \dots, \ell. \\ a & \text{if } j = \ell + 1. \\ y_j & \text{if } j = \ell + 2, \dots, 2\ell + 1. \\ u & \text{if } j = 2\ell + 2. \end{cases}$$

The vector space $P/Z(P)$ has a basis $\mathcal{B} = \{e_1, \dots, e_{2\ell}, e_{2\ell+1}, e_{2\ell+2}\}$ where $e_i = \overline{w}_i$ and the matrix of the alternating form b relatively to $\mathcal{B}$ is given by

$$\begin{pmatrix} 0 & I_{\ell+1} \\ I_{\ell+1} & 0 \end{pmatrix}.$$

We have to show that any automorphism σ in $Sp_\varphi(P/Z/(P))$ can be lifted to an automorphism $\tilde{\sigma}$ of P such that $\pi(\tilde{\sigma}) = \sigma$. Relatively to the basis $\mathcal{B}$, the automorphism σ is represented by a matrix $s = (s_{i,j})$ and we let

$$\tilde{\sigma}(w_j) = \prod_{i=1}^{2\ell+2} w_i^{s_{i,j}}.$$

With this definition, we have $\overline{\tilde{\sigma}(w_i)} = \sigma(\overline{w}_i)$ and furthermore

$$[\tilde{\sigma}(w_i), \tilde{\sigma}(w_j)] = b(\overline{\tilde{\sigma}(w_i)}, \overline{\tilde{\sigma}(w_j)}) = b(\sigma(\overline{w}_i), \sigma(\overline{w}_j)) = b(\overline{w}_i, \overline{w}_j) = [w_i, w_j].$$

To see that $\tilde{\sigma}$ defines an endomorphism of P, it remains to check that the orders are preserved. Since σ preserves φ, we have that σ stabilizes $\ker \varphi = \langle e_1, \dots, e_{2\ell+1} \rangle$. It follows that $s_{2\ell+2,j} = 0$ for $j = 1, \dots, 2\ell + 1$, and hence

$$\tilde{\sigma}(w_j) \in \Omega_1(P) = \langle w_1, \dots, w_{2\ell+1} \rangle, \text{ for all } j = 1, \dots, 2\ell + 1.$$

When p is odd, this shows that $\tilde{\sigma}(w_j)$ has order p for $j = 1, \dots 2\ell + 1$. When $p = 2$, $\tilde{\sigma}(w_j)$ may have order 4 for some $j \neq 2\ell + 2$. If it is the case, then we modify our definition of $\tilde{\sigma}(w_j)$ by letting

$$\tilde{\sigma}(w_j) = \left(\prod_{i=1}^{2\ell+2} w_i^{s_{i,j}} \right) \cdot w,$$

where $w = u^{2^{m-1}}$. Since $m > 1$, we have that w is central in P, so that all commuting relations are still preserved, but now $\tilde{\sigma}(w_j)$ has order 2, hence has the same order as w_j.

It remains to see that $w_{2\ell+2}$ has the same order as $\tilde{\sigma}(w_{2\ell+2})$. Since σ preserves φ, we have

$$\varphi(\overline{w}_{2\ell+2}) = \varphi(\sigma(\overline{w}_{2\ell+1})) = \varphi(\overline{\tilde{\sigma}(w_{2\ell+1})})$$

and it follows by definition of φ that $c = w_{2\ell+2}^p = \tilde{\sigma}(w_{2\ell+2})^p g$ with $g \in \mho^1(Z(P)) = \langle c^p \rangle$. Therefore $w_{2\ell+2}$ and $\tilde{\sigma}(w_{2\ell+2})$ have the same order.

It is easy now to see that $\tilde{\sigma}$ is an automorphism of P and we have also seen that $\pi(\tilde{\sigma}) = \sigma$. Therefore π is surjective on $Sp_\varphi(P/Z(P))$ so that the sequence is exact.

The last assertion concerning the isomorphism type of $Sp_\varphi(P/Z(P))$ can be found in Lemma 3.4.22. $\square$

Corollary 3.4.26. *Let $P = X_{p^{2\ell+1}} * M_{p^{m+2}}$ with $\ell \geq 0$ and $m > 1$. Then*

$$|\mathrm{Aut}(P)| = p^{(\ell+2)^2+m-2}(p-1)\prod_{i=1}^{\ell}(p^{2i}-1).$$

Remark 3.4.27. In the corresponding case $m = 1$, P is extraspecial of type II, that is $P = X_p^{*\ell} * X_{p^3}^-$. For such a group and according to Griess [15], the extension

$$1 \to \mathrm{Int}(P) \to \mathrm{Aut}_{Z(P)}(P) \to Sp_\varphi(P/Z(P)) \to 1$$

splits when p is odd. The argument seems to be similar to the one for extraspecial p-groups of type I, but in Griess' words, "...is technically more complicated.". No more details are given by Griess, but it is highly probable that the argument could be generalized to the case $m > 1$ when p is odd. We have no clue however of what happens when $p = 2$ and $m > 1$.

Automorphisms of p-groups with cyclic and non-central Frattini subgroup

So far, we have treated the case of p-groups with cyclic and central Frattini subgroup. Recall that if the Frattini subgroup of P is cyclic but not central, say of order 2^{m+1}, with $m > 1$, then $p = 2$ and P is isomorphic to $E \times (D_8^{*\ell} * S)$, with $\ell \geq 0$, and where E is elementary abelian and S is one of the groups in the following list:

$$D_{2^{m+2}}, SD_{2^{m+2}}, Q_{2^{m+2}}, D_{2^{m+3}}^+, Q_{2^{m+3}}^+, D_{2^{m+2}} * C_4, SD_{2^{m+2}} * C_4, D_{2^{m+3}}^+ * C_4. \tag{3.7}$$

In view of Lemma 3.4.1, we may assume that $E = 0$, so that $P = D_8^{*\ell} * S$, with S as in (3.7). In all cases, the subgroup $C_0 = C_P(\Phi(P))$ is maximal in P and $\Phi(C_0) = \Phi(P)$ is cyclic and central in C_0. More precisely, C_0 is isomorphic to

(I) $D_8^{*\ell} * C_{2^{m+1}}$, if S is isomorphic to $D_{2^{m+2}}$, $SD_{2^{m+2}}$, or $Q_{2^{m+2}}$;

(II) $D_8^{*\ell} * M_{2^{m+2}}$, if S is isomorphic to $D_{2^{m+3}}^+$ or $Q_{2^{m+3}}^+$;

(III) $(D_8^{*\ell} * C_{2^{m+1}}) \times C_2$, if S is isomorphic to $D_{2^{m+2}} * C_4$ or $SD_{2^{m+2}} * C_4$;

(IV) $(D_8^{*\ell} * M_{2^{m+2}}) \times C_2$, if S is isomorphic to $D_{2^{m+3}}^+ * C_4$.

The automorphism group of C_0 is thus known by our previous results. In what follows, we are going to describe the automorphism group of P mainly in terms of $\mathrm{Aut}(C_0)$. Since C_0 is characteristic in P, restriction of automorphisms induces a homomorphism

$$\rho : \mathrm{Aut}(P) \to \mathrm{Aut}(C_0).$$

In order to describe $\mathrm{Aut}(P)$, we are going to identify the image of ρ and its kernel, for all the possible choices of S. We will see in particular, that ρ is surjective, unless if $S = D_{2^{m+2}} * C_4$ or $S = SD_{2^{m+2}} * C_4$, in which case the image of ρ is a subgroup of index 2 in $\mathrm{Aut}(C_0)$.

Proposition 3.4.28. *Let $P = D_8^{*\ell} * S$, where S is one of the groups in the list (3.7). Let $C_0 = C_P(\Phi(P))$ and let $\rho : \mathrm{Aut}(P) \to \mathrm{Aut}(C_0)$ be the homomorphism induced by restriction of automorphisms.*

a) If $S = D_{2^{m+2}} * C_4$ or $S = SD_{2^{m+2}} * C_4$, then the image of ρ is the stabilizer of a cyclic subgroup of $Z(C_0)$ of maximal order. In particular, the image of ρ has index 2 in $\mathrm{Aut}(C_0)$.

b) In all other cases, ρ is surjective.

Proof. Let z be a generator of $Z(P)$ and let $x_1, y_1, \ldots, x_\ell, y_\ell$ be symplectic generators of the subgroup $D_8^{*\ell}$, all of order 2 and such that $[x_i, y_i] = z$, for $i = 1, \ldots, \ell$.

(I) Suppose first that S is one of the groups $D_{2^{m+2}}$, $SD_{2^{m+2}}$ or $Q_{2^{m+2}}$. Then S has two generators u and b, with u of order 2^{m+1}. The generator b has order 2 if S is $D_{2^{m+2}}$ or $SD_{2^{m+2}}$, and has order 4 if $S = Q_{2^{m+2}}$. The action of b on u is given by $bub^{-1} = u^{-1}$ if S is $D_{2^{m+2}}$ or $Q_{2^{m+2}}$, and is given by $bub^{-1} = u^{-1+2^m} = u^{-1}z$ if $S = SD_{2^{m+2}}$.

The subgroup C_0 is isomorphic to $D_8^{*\ell} * C_{2^{m+1}}$ and has the following generators

$$C_0 = \langle x_1, y_1, \ldots, x_\ell, y_\ell, u\rangle.$$

Let α be an automorphism of C_0. To show that ρ is surjective, we have to show that α can be extended to P, i.e. we have to define the value of α on the remaining generator b.

The center of C_0 is the cyclic subgroup of order 2^{m+1} generated by u, so that in particular $\alpha(u) = u^k$ for some odd k. The subgroup $\Omega_0 = \Omega_1(C_0)$ is characteristic in C_0, hence in P, and for $\ell \geq 1$, the group Ω_0 has the following generators, where $w = u^{2^{m-1}}$:

$$\Omega_0 = \langle x_1, y_1, \ldots, x_\ell, y_\ell, w\rangle.$$

In particular, we have

$$\alpha(x_i) = a_i w^{r_i} \tag{3.8}$$

for some $a_i \in \langle x_i, y_i, i = 1, \ldots, \ell\rangle$ and $r_i \in \{0, 1\}$. We have similarly

$$\alpha(y_i) = b_i w^{s_i} \tag{3.9}$$

for some $b_i \in \langle x_i, y_i, i = 1, \ldots, \ell\rangle$ and $s_i \in \{0, 1\}$.

To extend α to the whole group P, we let

$$\alpha(b) = \left(\prod_{i=1}^{\ell} \alpha(x_i)^{s_i} \alpha(y_i)^{r_i}\right) \cdot b. \tag{3.10}$$

If $\ell = 0$, we simply let $\alpha(b) = b$. To see that this extends α to an automorphism of P, we mainly have to check that, as defined, α is an endomorphism of P, the bijectivity of α being clear from the definition. We have thus to show that $\alpha(b)^2 = b^2$, that the action of b on u is preserved and that the relations $[b, x_i] = 1$ and $[b, y_i] = 1$ are preserved for $i = 1, \ldots, \ell$. The other relations defining P are expressed inside C_0, hence are automatically preserved since α is an endomorphism of C_0.

We consider first the relation $[b, x_i] = 1$. It is useful to note here that the subgroup generated by b and w is isomorphic to D_8, since $bwb^{-1} = w^{-1} = wz$. The subgroup generated by Ω_0 and b has thus a central Frattini subgroup of order 2, namely $Z(P)$. It follows that commutators can be computed easily (see Lemma 1.2.1). We have

$$\begin{aligned} [\tilde{\alpha}(b), \tilde{\alpha}(x_i)] &= [\prod_{j=1}^{\ell} \alpha(x_j)^{s_j} \alpha(y_j)^{r_j} b, \alpha(x_i)] = [\alpha(y_i)^{r_i} b, \alpha(x_i)] \\ &= [\alpha(y_i), \alpha(x_i)]^{r_i} [b, a_i w^{r_i}] = \alpha([x_i, y_i]^{r_i}) \cdot [b, w^{r_i}] \\ &= z^{r_i} \cdot z^{r_i} = 1. \end{aligned} \tag{3.11}$$

Therefore the relations $[b, x_i] = 1$, $i = 1, \ldots, \ell$, are preserved and a similar argument shows that the relations $[b, y_i] = 1$ are also preserved.

Since α is an endomorphism of C_0, we have that $\alpha(x_i)$ and $\alpha(y_i)$ commute with $\alpha(u)$, for all $i = 1, \ldots, \ell$. It follows that the action of $\alpha(b)$ on $\alpha(u) = u^k$ is the same as the action of b on $\alpha(u)$, hence the relation given by the action of b on u is preserved.

It remains thus to see that $\alpha(b)^2 = b^2$. Let $r = \sum_{i=1}^{\ell} r_i s_i$, we have first

$$\prod_{i=1}^{\ell} \alpha(x_i)^{s_i} \alpha(y_i)^{r_i} = \prod_{i=1}^{\ell} (a_i w^{r_i})^{s_i} (b_i w^{s_i})^{r_i} = \prod_{i=1}^{\ell} a_i^{s_i} w^{r_i s_i} b_i^{r_i} w^{r_i s_i} = \prod_{i=1}^{\ell} a_i^{s_i} b_i^{r_i} z^r.$$

It follows now from Lemma 1.2.2 that

$$\left(\alpha(b)\right)^2 = \left(\prod_{i=1}^{\ell} a_i^{s_i} b_i^{r_i} z^r\right)^2 \cdot b^2 \cdot [b, \prod_{i=1}^{\ell} a_i^{s_i} b_i^{r_i} z^r] = z^r b^2$$

To see that $\alpha(b)^2 = b^2$, we are thus led to check that $r = \sum_{i=1}^{\ell} r_i s_i = 0$. For this, note that the group Ω_0 is isomorphic to $D_8^{*\ell} * C_4$ and hence the quotient $V = \Omega_0 / Z(P)$ is a quadratic space endowed with the quadratic form q given by $q(\overline{x}) = x^2 \in \Phi(\Omega_0)$. The polar form of q is the alternating form b induced by commutators so that in particular $V = W \oplus V^{\perp}$, where $V^{\perp}$ is the one-dimensional subspace of V generated by the class of w in V. The automorphism $\overline{\alpha}$ induced by α on V preserves the quadratic form since α is the identity on $\Phi(\Omega_0) = Z(P)$.

The vector space V has a basis $\mathcal{B}$ given by the images in V of the elements x_i, y_i, $i = 1, \ldots, \ell$, and w. It follows from (3.8) and (3.9) that the matrix of α

relatively to the basis $\mathcal{B}$ has the following form:

$$\left(\begin{array}{ccccc|c} & & & & & 0 \\ & & A & & & \vdots \\ & & & & & 0 \\ \hline r_1 & s_1 & \cdots & r_\ell & s_\ell & 1 \end{array}\right)$$

and is in the orthogonal group $O(2\ell+1,2)$ since α preserve q. It follows now from a general result on the orthogonal group $O(2\ell+1,2)$ (see Proposition B.0.22 in Appendix B) that $\sum_{i=1}^{\ell} r_i s_i = 0$.

(II) Suppose now that S is the group $D^+_{2^{m+3}}$ or the group $Q^+_{2^{m+3}}$. Let a, b and u be generators of S such that u has order 2^{m+1}, a has order 2, $aua^{-1} = u^{1+2^m} = uz$, $bub^{-1} = u^{-1}$ and a and b commute. The generator b has order 2 if $S = D^+_{2^{m+3}}$, and has order 4 if $S = Q^+_{2^{m+3}}$.

The subgroup C_0 of P has the following generators

$$C_0 = \langle x_1, y_1, \ldots, x_\ell, y_\ell, u, a\rangle$$

and is isomorphic to $D_8^{*\ell} * M_{2^{m+2}}$. The subgroup $\Omega_0 = \Omega_1(C_0)$ is characteristic in C_0, hence in P and, for $\ell \geq 1$, has the following generators

$$\Omega_0 = \langle x_1, y_1, \ldots, x_\ell, y_\ell, w, a\rangle,$$

where $w = u^{2^{m-1}}$. It follows that

$$\alpha(x_i) = a_i w^{r_i}, \tag{3.12}$$

for some $a_i \in \langle x_1, y_1, \ldots, x_\ell, y_\ell, a\rangle$ and $r_i \in \{0,1\}$. We have similarly

$$\alpha(y_i) = b_i w^{s_i}, \tag{3.13}$$

for some $b_i \in \langle x_1, y_1, \ldots, x_\ell, y_\ell, a\rangle$ and $s_i \in \{0,1\}$.

We have also $\alpha(u) = u^k x a^\varepsilon$, for some odd k, $x \in \langle x_i, y_i, i = 1, \cdots, \ell\rangle$ and $\varepsilon \in \{0,1\}$. Since the subgroup $\Omega_1(Z(\Omega_0)) = \langle z, a\rangle$ is characteristic in C_0, we have $\alpha(a) = a$ or $\alpha(a) = az$. To extend α to an automorphism of P, it remains to choose its value on the generator b. We let

$$\alpha(b) = \left(\prod_{i=1}^{\ell} \alpha(x_i)^{s_i} \alpha(y_i)^{r_i}\right) \cdot b. \tag{3.14}$$

If $\ell = 0$, we simply let $\alpha(b) = b$. We have to check that this definition preserves the relations defining P. We only have to check that $\alpha(b)^2 = b^2$ and that the following relations are preserved:

$$\begin{gathered} bub^{-1} = u^{-1}, \\ [b, x_i] = [b, y_i] = 1, \text{ for all } i = 1, \ldots, \ell, \\ [b, a] = 1. \end{gathered}$$

The other relations are defined inside C_0 and are immediately preserved since α is an endomorphism of C_0. It is almost immediate that the relation $[b,a] = 1$

is preserved, since $\alpha(x_i)$ and $\alpha(y_i)$ commute with a, for all $i = 1, \ldots, \ell$. The verification that the relations $[b, x_i] = [b, y_i] = 1$ are preserved is identical to the one performed in the previous case in (3.11).

We consider now the action of b on u. We have to verify that

$$\alpha(b)\alpha(u)\alpha(b)^{-1} = \alpha(u)^{-1}.$$

Since α is an endomorphism of C_0, we have that $\alpha(x_i)$ and $\alpha(y_i)$ commute with $\alpha(u)$, for all $i = 1, \ldots, \ell$. We have then

$$\alpha(b)\alpha(u)\alpha(b)^{-1} = b\alpha(u)b^{-1} = b(u^k xa^\varepsilon)b^{-1} = u^{-k}xa^\varepsilon.$$

We have now

$$(\alpha(b)\alpha(u)\alpha(b)^{-1})\alpha(u) = (u^{-k}xa^\varepsilon)(u^k xa^\varepsilon) = z^\varepsilon x^2.$$

Since $x^2 \in \langle z \rangle$, we have either $z^\varepsilon x^2 = 1$, or $z^\varepsilon x^2 = z$. If we are in this second case, namely $z^\varepsilon x^2 = z$, then we modify our initial definition of $\alpha(b)$ by choosing instead

$$\alpha(b) = \left(\prod_{i=1}^{\ell} \alpha(x_i)^{s_i} \alpha(y_i)^{r_i} \right) \cdot ba. \tag{3.15}$$

In this way, we introduce, if needed, the element a in $\alpha(b)$ in order to have $\alpha(b)\alpha(u)\alpha(b)^{-1} = \alpha(u)^{-1}$, so that the relation $bub^{-1} = u^{-1}$ is preserved. Note that since a is central in Ω_0, the relations $[b, x_i] = [b, y_i] = 1$ and $[b, a] = 1$ are still preserved after the modification performed in (3.15).

It remains now to see that $\alpha(b)^2 = b^2$. This is done in a manner similar to what was performed in the previous case with only small changes, that we indicate now. The first difference is that, in some cases, $\alpha(b)$ has to be modified by the element a as in (3.15). But this change has no incidence on the value of $\alpha(b)^2$, since a has order 2, is central in Ω_0 and commutes with b. The second difference is that here Ω_0 is isomorphic to $(D_8^{*\ell} * C_4) \times C_2$ and we have have to consider then the quadratic space $V = \Omega_0/\Omega_1(Z(\Omega_0))$, which has a symplectic basis induced by w and the generators x_i, y_i, for $i = 1, \ldots, \ell$. The rest of the argument is then identical to the one in the previous case.

(III) Suppose now that $S = D_{2^{m+2}} * C_4$ or $S = SD_{2^{m+2}} * C_4$. Let u, b and c be generators of S, such that c is central in S with $c^2 = z$, the generator u has order 2^{m+1} and b has order 2. We will assume that $S = D_{2^{m+2}} * C_4$, so that $bub^{-1} = u^{-1}$. The other case, namely $S = SD_{2^{m+2}} * C_4$, can be treated similarly.

In this situation, the group C_0 has the following generators

$$C_0 = \langle x_1, y_1, \ldots, x_\ell, y_\ell, u, c \rangle$$

and is isomorphic to $D_8^{*\ell} * C_{2^{m+1}} * C_4 \cong (D_8^{*\ell} * C_{2^{m+1}}) \times C_2$. The subgroup $Z_0 = Z(C_0)$ is generated by u and c, is characteristic in P and has two cyclic subgroups of maximal order, namely $\langle u \rangle$ and $\langle uc \rangle$. The automorphism group of P acts on these two subgroups and we show first that any automorphism of P stabilizes $\langle u \rangle$.

Supppose by contradiction that $\beta \in \mathrm{Aut}(P)$ does not centralize $\langle u \rangle$. We have then that $\beta(u) = u^k c$, for some odd k. Since C_0 is a characteristic subgroup of index 2 in P and $b \notin C_0$, we have $\beta(b) \in bC_0$. Since $\beta(u) \in Z_0$ is obviously central in C_0, we have thus

$$\beta(bub^{-1}) = \beta(b)\beta(u)\beta(b)^{-1} = b\beta(u)b^{-1} = b(u^k c)b^{-1} = u^{-k}c.$$

But this is a contradiction, since $\beta(bub^{-1}) = \beta(u^{-1}) = \beta(u)^{-1} = u^{-k}c^{-1}$. Any automorphism of P must then stabilize $\langle u\rangle$, that is, must stabilize the cylic subgroups of maximal order in Z_0.

We show next that any automorphism α of C_0 that stabilizes $\langle u\rangle$ can be extended to an automorphism of the whole group P. For $\ell \geq 1$, the subgroup $\Omega_0 = \Omega_1(C_0)$ has the following generators

$$\Omega_0 = \langle x_1, y_1, \dots, x_\ell, y_\ell, w, c\rangle,$$

and is isomorphic to $(D_8^{*\ell} * C_4) \times C_2$. Similarly to the previous cases, we have then $\alpha(x_i) = a_i w^{r_i}$ and $\alpha(y_i) = b_i w^{s_i}$, with $a_i, b_i \in \langle x_1, y_1, \dots, x_\ell, y_\ell, c\rangle$. The subgroup $\Omega_1(Z(\Omega_0)) = \langle z, c\rangle$ is characteristic in P, so that $\alpha(c) = c$ or $\alpha(c) = cz$. The automorphism $\alpha \in \mathrm{Aut}(C_0)$ can now be extended to b exactly as in (3.10), that is,

$$\alpha(b) = \left(\prod_{i=1}^{\ell} \alpha(x_i)^{s_i}\alpha(y_i)^{r_i}\right) \cdot b. \tag{3.16}$$

If $\ell = 0$, we simply let $\alpha(b) = b$. The verifications that the relations

$$[b, x_i] = [b, y_i] = 1, \text{ for all } i = 1, \dots, \ell,$$

are preserved can be done similarly to what was performed in the first case of the proof. The only change is the eventual presence of the generator c, but this does not have any incidence on the argument, since c is central. Since α stabilizes $\langle u\rangle$, we have $\alpha(u) = u^k$, for some odd k and the verification that the relation

$$bub^{-1} = u^{-1}$$

is preserved can also be done similarly to what was performed in the first case of the proof. It is easy to see that the relation $[c, b] = 1$ is preserved and it remains to see that $\alpha(b)$ has order 2. For this, an argument similar to the one used in the first case of the proof can be used, but there is however a much easier argument in this situation. Indeed, if $\alpha(b)^2 = z$, then we modify our initial definition of $\alpha(b)$ by letting

$$\alpha(b) = \left(\prod_{i=1}^{\ell} \alpha(x_i)^{s_i}\alpha(y_i)^{r_i}\right) \cdot bc.$$

instead of (3.16), so that now $\alpha(b)^2 = 1$.

(IV) Suppose now that $S = D^+_{2^{m+3}} * C_4$. Let a, b, u and c be generators of S, where c is central in S with $c^2 = z$, u has order 2^{m+1}, a and b have order 2, $aua^{-1} = uz$ and $bub^{-1} = u^{-1}$. The subgroup C_0 has the following generators

$$C_0 = \langle x_1, y_1, \dots, x_\ell, y_\ell, a, u, c\rangle$$

and is isomorphic to $D_8^{*\ell} * M_{2^{m+2}} * C_4 \cong (D_8^{*\ell} * M_{2^{m+2}}) \times C_2$. Similarly to the previous cases, we have $\alpha(x_i) = a_i w^{r_i}$ and $\alpha(y_i) = b_i w^{s_i}$, where a_i, b_i are elements of the subgroup $\langle x_1, y_1, \ldots, x_\ell, y_\ell, a, c\rangle$, for all $i = 1, \ldots, \ell$. We let

$$\alpha(b) = \left(\prod_{i=1}^{\ell} \alpha(x_i)^{s_i} \alpha(y_i)^{r_i}\right) \cdot b. \tag{3.17}$$

We have $\alpha(u) = u^k x a^\varepsilon c^\delta$, for some odd k, and with $x \in \langle x_i, y_i, i = 1, \cdots, \ell\rangle$ and $\varepsilon, \delta \in \{0, 1\}$. The action of $\alpha(b)$ on $\alpha(u)$ is given by

$$\alpha(b)\alpha(u)\alpha(b)^{-1} = b\alpha(u)b^{-1} = b(u^k x a^\varepsilon)c^\delta b^{-1} = u^{-k} x a^\varepsilon c^\delta.$$

We have now

$$(\alpha(b)\alpha(u)\alpha(b)^{-1})\alpha(u) = (u^{-k} x a^\varepsilon c^\delta)(u^k x a^\varepsilon c^\delta) \in \langle z\rangle.$$

If $(\alpha(b)\alpha(u)\alpha(b)^{-1})\alpha(u) = z$, then we modify the initial definition (3.17) of $\alpha(b)$ by letting

$$\alpha(b) = \left(\prod_{i=1}^{\ell} \alpha(x_i)^{s_i} \alpha(y_i)^{r_i}\right) \cdot ba.$$

As defined, α preserves the relation $bub^{-1} = u^{-1}$. The element $\alpha(b)$ can be modified by c, if needed, in order to have $\alpha(b)^2 = 1$. The verification that the other relations are preserved is similar to the one performed in the previous cases. $\square$

We are now in position to describe the automorphism groups of p-groups with a cyclic but non-central Frattini subgroup. Recall that this implies $p = 2$ and that we may assume that the center of P is cyclic, so that $P = D_8^{*\ell} * S$, where S is one of the following groups:

$$D_{2^{m+2}}, SD_{2^{m+2}}, Q_{2^{m+2}}, D^+_{2^{m+3}}, Q^+_{2^{m+3}}, D_{2^{m+2}} * C_4, SD_{2^{m+2}} * C_4, D^+_{2^{m+3}} * C_4. \tag{3.18}$$

Proposition 3.4.29. *Let $P = D_8^{*\ell} * S$ with S taken in the list (3.18). If $S = D_{2^{m+2}} * C_4$ or $S = SD_{2^{m+2}} * C_4$, then there is an exact sequence*

$$1 \to \mathrm{Aut}_{C_0}(P) \to \mathrm{Aut}(P) \to A \to 1,$$

where A is a subgroup of index 2 of $\mathrm{Aut}\, C_0$. More precisely, A is the stabilizer in $\mathrm{Aut}(C_0)$ of a cyclic subgroup of maximal order in $Z(C_0)$. In all other cases, there is an exact sequence

$$1 \to \mathrm{Aut}_{C_0}(P) \to \mathrm{Aut}(P) \to \mathrm{Aut}(C_0) \to 1.$$

Furthermore, in all cases, $\mathrm{Aut}_{C_0}(P)$ is cyclic and more precisely, $\mathrm{Aut}_{C_0}(P)$ has order 2^{m+1} if S is one of the following groups:

$$D_{2^{m+2}}, Q_{2^{m+2}}, D_{2^{m+2}} * C_4, SD_{2^{m+2}} * C_4;$$

and has order 2^m if S is one of the following groups:

$$SD_{2^{m+2}}, D^+_{2^{m+3}}, Q^+_{2^{m+3}}, D^+_{2^{m+3}} * C_4.$$

Proof. We have seen in the previous proposition that the homomorphism $\rho : \mathrm{Aut}(P) \to \mathrm{Aut}(C_0)$ is surjective. It is immediate that $\ker\rho$ is the group $\mathrm{Aut}_{C_0}(P)$ and we obtain thus the desired exact sequence. It remains to determine more precisely this group $\mathrm{Aut}_{C_0}(P)$ for each of the groups in the list (3.18).

Let z be a generator of $Z(P)$ and let $x_1, y_1, \ldots, x_\ell, y_\ell$ be symplectic generators of the subgroup $D_8^{*\ell}$, all of order 2 and such that $[x_i, y_i] = z$, for $i = 1, \ldots, \ell$.

Suppose first $S = D_{2^{m+2}}$ and let b, u be generators of S with u of order 2^{m+1}, b of order 2 and $bub^{-1} = u^{-1}$. Let $\alpha \in \mathrm{Aut}_{C_0}(P)$. Since C_0 is characteristic in P and P/C_0 has order 2, we have $\alpha(b) \in bC_0$, hence

$$\alpha(b) = bu^k x$$

for some k and some $x \in \langle x_i, y_i, i = 1, \ldots, \ell\rangle$. If x is not in $Z(P)$, then there exists $y \in \langle x_i, y_i, i = 1, \ldots, \ell\rangle$ such that $[x, y] = z$. Since $\langle x_i, y_i, i = 1, \ldots, \ell\rangle$ is contained in C_0, we have $\alpha(y) = y$, so that

$$\alpha([b, y]) = [\alpha(b), \alpha(y)] = [bu^k x, y] = [x, y] = z$$

which is a contradiction, since $[b, y] = 1$. It follows that x must be in $Z(P)$, hence $\alpha(b) = bu^k$ for some k, since $z = u^{2^m}$. The group $\mathrm{Aut}_{C_0}(P)$ is thus generated by the automorphism μ of P_0 defined by $\mu(b) = bu$ and by the identity on C_0. Since $\mu^k(b) = bu^k$, we have that μ has order 2^{m+1}, so that $\mathrm{Aut}_{C_0}(P)$ is cyclic of order 2^{m+1}.

The case $S = Q_{2^{m+2}}$ is identical to the previous case. For $S = SD_{2^{m+2}}$, the situation is analogous, with the difference that the generator of $\mathrm{Aut}_{C_0}(P)$ is defined then by $\mu(b) = bu^{-2}$, since bu^i has not order 2 if i is odd. It follows that for $S = SD_{2^{m+2}}$, the group $\mathrm{Aut}_{C_0}(P)$ is cyclic of order 2^m.

Suppose now $S = D^+_{2^{m+3}}$ and let u, b, a be generators of S, with u of order 2^{m+1}, a and b of order 2 and such that $[a, b] = 1$, $aua^{-1} = uz$ and $bub^{-1} = u^{-1}$. We have

$$\alpha(b) = bu^k x a^\varepsilon,$$

for some k, $\varepsilon \in \{0, 1\}$ and $x \in \langle x_i, y_i, i = 1, \ldots, \ell\rangle$. The same argument as above shows that x must be in $Z(P)$, so that we may assume $x = 1$. Furthermore, since u is fixed by α, the action of $\alpha(b)$ on u must be the same as the action of b on u, so that we must have $\varepsilon = 0$ and hence

$$\alpha(b) = bu^k$$

for some k. Since a and b commutes and a is fixed by α, we must also have that $\alpha(b)$ commutes with a, so that k must be even. The subgroup $\mathrm{Aut}_{C_0}(P)$ is thus generated by the automorphism μ of P defined by $\mu(b) = bu^2$ and by the identity on C_0. It follows that $\mathrm{Aut}_{C_0}(P)$ is cyclic of order 2^m. The same argument shows the same result if $S = Q^+_{2^{m+3}}$.

Suppose now $S = D_{2^{m+2}} * C_4$. Let b, u be generators of the subgroup $D_{2^{m+2}}$ as above and let c be a generator of the central subgroup C_4. If α is an automorphism of P acting as the identity on C_0, then the same arguments as above show that

$$\alpha(b) = bu^k c^\delta$$

for some k and δ. Since c has order 4 and commutes with b and u, we must have $c^\delta \in \langle z\rangle$, so that $\alpha(b) = bu^k$ for some k. It follows that $\mathrm{Aut}_{C_0}(P)$ is cyclic of order 2^{m+1} generated by the automorphism of P sending b to bu and acting as the identity on C_0.

If $S = SD_{2^{m+2}} * C_4$, then for identical reasons, we have $\alpha(b) = bu^k c^\delta$. But since bu^k may have order 4, we don't have necessarily that c^δ is in $\langle z\rangle$. In fact, $\mathrm{Aut}_{C_0}(P)$ is cyclic of order 2^{m+1} generated by the automorphism sending b to buc and acting as the identity on C_0.

The case $S = D^+_{2^{m+3}} * C_4$ is similar to the above treated case $S = D^+_{2^{m+3}}$. In this situation, $\mathrm{Aut}_{C_0}(P)$ is cyclic of order 2^m generated by the automorphism of P sending b to bu^2 and acting as the identity on C_0. □

Corollary 3.4.30. *Let $P = D_8^{*\ell} * S$, with S as in (3.18).*

a) If $S = D_{2^{m+2}}$ or $S = Q_{2^{m+2}}$, then

$$|\mathrm{Aut}(P)| = 2^{(\ell+1)^2+2m}\prod_{i=1}^{\ell}(2^{2i}-1).$$

b) If $S = SD_{2^{m+2}}$, then

$$|\mathrm{Aut}(P)| = 2^{(\ell+1)^2+2m-1}\prod_{i=1}^{\ell}(2^{2i}-1).$$

c) If $S = D^+_{2^{m+3}}$ or $S = Q^+_{2^{m+3}}$, then

$$|\mathrm{Aut}(P)| = 2^{(\ell+2)^2+2m-2}\prod_{i=1}^{\ell}(2^{2i}-1).$$

d) If $S = D_{2^{m+2}} * C_4$ or $S = SD_{2^{m+2}} * C_4$, then

$$|\mathrm{Aut}(P)| = 2^{(\ell+2)^2+2m-2}\prod_{i=1}^{\ell}(2^{2i}-1).$$

e) If $S = D^+_{2^{m+3}} * C_4$, then

$$|\mathrm{Aut}(P)| = 2^{(\ell+3)^2+2m-4}\prod_{i=1}^{\ell}(2^{2i}-1).$$

Proof. The exact sequence

$$1 \to \mathrm{Aut}_{C_0}(P) \to \mathrm{Aut}(P) \to \mathrm{Aut}(C_0) \to 1$$

shows in particular that $|\mathrm{Aut}(P)| = |\mathrm{Aut}_{C_0}(P)| \cdot |\mathrm{Aut}(C_0)|$. The order of $\mathrm{Aut}_{C_0}(P)$ can be found in Proposition 3.4.29 and the order of $\mathrm{Aut}(C_0)$ can be deduced from Corollary 3.4.3, Corollary 3.4.12 and Corollary 3.4.26. □

3.5 Automorphisms of p-groups of class 2 with cyclic center

In this section, p will always denote an odd prime number. Let P be a p-group of class 2 with a cyclic center and such that $P/Z(P)$ is homocyclic. The description of the automorphism group of such groups is very similar to the description for p-groups with cyclic and central Frattini subgroup performed previously. As a first step, we show that the problem can be reduced to the study of automorphisms fixing the center pointwise.

We fix a p-group P of class 2 with a cyclic center and such that $P/Z(P)$ is homocyclic of type p^m, $m \geq 1$. Recall from Lemma 1.4.1 that p^m is also the order of the derived subgroup P' of P. The group P is isomorphic to one of the following groups

1. $P = X_3(p^m)^{*\ell} * C_{p^{m+r}}$, with $\ell \geq 1$ and $r \geq 0$.
2. $P = X_3(p^m)^{*(\ell-1)} * M(m,s)$, with $\ell \geq 1$ and $s \geq 1$.
3. $P = X_3(p^m)^{*(\ell-1)} * M(m,s) * C_{p^{m+r}}$, with $\ell \geq 1$ and $1 \leq r < s < m+r$.

We will treat these three cases separately, but before we briefly recall the definition of the alternating form and the linear form on $P/Z(P)$. We denote by $V = P/Z(P)$ and for $x \in P$ we denote by $\overline{x}$ its class in V. Let z be a generator of $Z(P)$ and $c = z^{p^r}$ be a generator of P', the map

$$b : V \times V \to \mathbb{Z}/p^m\mathbb{Z}$$

defined by $[x,y] = c^{b(\overline{x},\overline{y})}$ is a non-degenerate alternating form on the free $\mathbb{Z}/p^m\mathbb{Z}$-modulo $P/Z(P)$. In order to simplify the notation, we will sometimes use $b(\overline{x},\overline{y})$ also to denote the element $[x,y]$.

The map

$$\varphi : V \to \mathbb{Z}/p^m\mathbb{Z}$$

defined by $x^{p^m} = \pi(z)^{\varphi(\overline{x})}$, where π is the canonical homomorphism $Z(P) \to Z(P)/\mho^m(P)$, is a linear form on V.

Automorphisms of $X_{2\ell+1}(p^m) * C_{p^{m+r}}$

Let $P = X_3(p^m)^{*\ell} * C_{p^{m+r}}$ with $\ell \geq 1$, $m \geq 1$ and $r \geq 0$. Note that when $r = 0$, P is simply the group $X_3(p^m)^{*\ell} = X_{2\ell+1}(p^m)$. Let z be a generator of $Z(P)$. The group P is generated by z and elements $x_1, y_1, \ldots, x_\ell, y_\ell$ all of order p^m and satisfying

$$[x_i, y_i] = z^{p^r}, \text{ for all } 1 \leq i \leq \ell.$$
$$[x_i, x_j] = [x_i, y_j] = [y_i, y_j] = 1, \text{ for all } 1 \leq i \neq j \leq \ell.$$

Lemma 3.5.1. *The following sequence is exact and splits*

$$1 \to \mathrm{Aut}_{Z(P)}(P) \to \mathrm{Aut}(P) \to \mathrm{Aut}(Z(P)) \to 1.$$

Proof. It is enough to show that there exists a homomorphic section. If α is an automorphism of $Z(P)$, then $\alpha(z) = z^k$ for some k prime to p and uniquely determined modulo p^{m+r}. We extend α to an automorphism $\tilde{\alpha}$ of P by letting

$$\begin{aligned} \tilde{\alpha}(z) &= \alpha(z) = z^k. \\ \tilde{\alpha}(x_i) &= x_i, \text{ for all } 1 \leq i \leq \ell. \\ \tilde{\alpha}(y_i) &= y_i^k, \text{ for all } 1 \leq i \leq \ell. \end{aligned}$$

All relations are preserved and k is prime to p, so that $\tilde{\alpha}$ is an automorphism of P. The definition of $\tilde{\alpha}$ does not depend on the choice of k modulo p^{m+r} so that the map sending an automorphism α of $Z(P)$ to the automorphism $\tilde{\alpha}$ of P is a homomorphism. This shows that the sequence splits and the lemma is proved. □

From now on, we identify $\mathrm{Aut}(Z(P))$ to a subgroup of $\mathrm{Aut}(P)$. If α is an automorphism of $Z(P)$, we will also use α to denote its extension to an automorphism of the whole group P.

Since $Z(P)$ is characteristic, there is a canonical homomorphism

$$\pi : \mathrm{Aut}_{Z(P)}(P) \to \mathrm{Aut}(P/Z(P)).$$

We denote by $Sp(P/Z(P))$ the subgroup of $\mathrm{Aut}(P/Z(P))$ consisting of all automorphisms preserving b, namely

$$Sp(P/Z(P)) = \{\alpha \in \mathrm{Aut}(P/Z(P)) \,|\, b(\alpha v, \alpha w) = b(v, w), \forall v, w \in P/Z(P)\}.$$

Choosing a basis of the free $\mathbb{Z}/p^m\mathbb{Z}$-module $P/Z(P)$, we can identify the groups $Sp(P/Z(P))$ and $Sp(2\ell, \mathbb{Z}/p^m\mathbb{Z})$. The following lemma shows that automorphisms of P fixing $Z(P)$ pointwise preserve the alternating form b, hence are in $Sp(P/Z(P))$.

Lemma 3.5.2. *The image of π is contained in $Sp(P/Z(P))$.*

Proof. If α is an automorphism of P fixing $Z(P)$ pointwise, then by definition $\pi(\alpha)(\overline{x}) = \overline{\alpha(x)}$ and thus

$$b(\overline{x}, \overline{y}) = [x, y] = \alpha([x, y]) = [\alpha x, \alpha y] = b(\overline{\alpha(x)}, \overline{\alpha(y)}) = b(\pi(\alpha)(\overline{x}), \pi(\alpha)(\overline{y})).$$

Therefore $\pi(\alpha)$ preserves the non-degenerate alternating form b induced by the commutators. □

Lemma 3.5.3. *The kernel of π is equal to the group $\mathrm{Int}(P)$ of inner automorphisms of P.*

Proof. The kernel of π consists of all automorphisms of P fixing $Z(P)$ and $P/Z(P)$ pointwise. It follows from Lemma 3.2.1 that $\ker \pi$ is isomorphic to $\mathrm{Hom}(P/Z(P), Z(P))$. But $Z(P)$ is cyclic of order p^{m+r} and $P/Z(P)$ is a direct product of 2ℓ copies of the cyclic group p^m, hence

$$\ker \pi \cong \mathrm{Hom}((C_{p^m})^{2\ell}, C_{p^{m+r}}) \cong \mathrm{Hom}((C_{p^m})^{2\ell}, C_{p^m}) \cong (C_{p^m})^{2\ell}.$$

Since also $\mathrm{Int}(P) \cong P/Z(P) \cong (C_{p^m})^{2\ell}$, it is enough to check that $\mathrm{Int}(P)$ is contained in $\ker\pi$. It is clear that any inner automorphism of P fixes $Z(P)$ pointwise. Since P' is central in P, we also have $c_x(y) \in yZ(P)$ for any $x, y \in P$. It follows that c_x induces the identity on $P/Z(P)$ and therefore $\mathrm{Int}(P) \leq \ker\pi$ and the lemma is proved. □

Proposition 3.5.4. *Let $P = X_{2\ell+1}(p^m) * C_{p^{m+r}}$ with $\ell \geq 1$, $m \geq 1$ and $r \geq 0$. Then*

$$\mathrm{Aut}(P) = \mathrm{Aut}_{Z(P)}(P) \rtimes \mathrm{Aut}(Z(P))$$

and there is a short exact sequence

$$1 \to \mathrm{Int}(P) \to \mathrm{Aut}_{Z(P)}(P) \to Sp(2\ell, \mathbb{Z}/p^m\mathbb{Z}) \to 1.$$

Proof. In view of the previous lemmas, it remains only to check that the map $\pi : \mathrm{Aut}_{Z(P)}(P) \to \mathrm{Aut}(P/Z(P))$ is surjective on $Sp(P/Z(P))$. To begin, we reorder the elements $x_1, y_1, \ldots, x_\ell, y_\ell$. For $j = 1, \ldots, \ell$ we let $w_j = x_j$ and $w_{j+\ell} = y_j$. We have this way

$$[w_i, w_j] = \begin{cases} z^{p^r} & \text{if } |i-j| = \ell. \\ 1 & \text{else.} \end{cases}$$

We will show that any automorphism of $P/Z(P)$ preserving b is induced by an automorphism of P. So let α be an automorphism of $P/Z(P)$ such that $\alpha(b(v, w)) = b(\alpha v, \alpha w)$ for all $v, w \in P/Z(P)$. For any $x \in P$ we denote by $\overline{x}$ its class in $P/Z(P)$. We have then for all $i = 1, \ldots, 2\ell$

$$\alpha(\overline{w}_i) = \overline{w}_1^{s_{1,i}} \cdots \overline{w}_{2\ell}^{s_{2\ell,i}}.$$

We define now $\tilde{\alpha} : P \to P$ to be the map with the following values on the generators of P

$$\begin{aligned} \tilde{\alpha}(z) &= z, \\ \tilde{\alpha}(w_i) &= w_1^{s_{1,i}} \cdots w_{2\ell}^{s_{2\ell,i}}. \end{aligned}$$

With this definition, we have $\overline{\tilde{\alpha}(w_i)} = \alpha(\overline{w}_i)$ and since α preserves b we have now for all $1 \leq i, j \leq 2\ell$

$$[\tilde{\alpha}(w_i), \tilde{\alpha}(w_j)] = b(\overline{\tilde{\alpha}(w_i)}, \overline{\tilde{\alpha}(w_j)}) = b(\alpha(\overline{w_i}), \alpha(\overline{w_j})) = b(\overline{w_i}, \overline{w_j}) = [w_i, w_j].$$

Since α is invertible, for all $1 \leq i \leq 2\ell$ there exists j such that $s_{j,i}$ is prime to p. It follows from Lemma 1.4.2 that $\tilde{\alpha}(w_i)$ has order p^m and therefore $\tilde{\alpha}$ is an endomorphism of P. Since α is an automorphism, $\tilde{\alpha}$ is also invertible hence $\tilde{\alpha}$ is an automorphism of P. It is clear that $\tilde{\alpha}$ induces α on $P/Z(P)$. It follows that π is surjective on the subgroup of $\mathrm{Aut}(P/Z(P))$ consisting of automorphisms preserving the non-degenerate alternating form b, that is $\mathrm{Im}\,\psi$ is isomorphic to the group $Sp_{2\ell}(\mathbb{Z}/p^m\mathbb{Z})$. □

Automorphisms of $X_{2(\ell-1)+1}(p^m) * M(m,s)$

Let $P = X_3(p^m)^{*(\ell-1)} * M(m,s)$ with $\ell \geq 1$ and $s \geq 1$ and let z be a generator of $Z(P)$. Recall that $Z(P)$ has order $p^{\max\{m,s\}}$. The group P is generated by z and elements $x_1, y_1, \ldots, x_\ell, y_\ell$ such that all except y_ℓ have order p^m and satisfy

$$[x_i, y_i] = z.$$
$$[x_i, x_j] = [x_i, y_j] = [y_i, y_j] = 1.$$

Furthermore, we have

$$y_\ell^{p^m} = \begin{cases} z^{p^{m-s}} & \text{if } s \leq m. \\ z & \text{if } m \leq s. \end{cases}$$

Let U be the subgroup generated by y_ℓ. This is a cyclic subgroup of P of order p^{m+s} containing P'.

Lemma 3.5.5. *There is an injective homomorphism*

$$\mathrm{Aut}(U) \hookrightarrow \mathrm{Aut}(P).$$

Proof. An automorphism $\alpha \in \mathrm{Aut}(U)$ sends y_ℓ to y_ℓ^k for some k prime to p and uniquely defined modulo p^{m+s}. We extend α to the whole group P by letting

$$\tilde{\alpha}(x_i) = x_i,$$
$$\tilde{\alpha}(y_i) = y_i^k,$$
$$\tilde{\alpha}(z) = z^k.$$

As defined, $\tilde{\alpha}$ preserves all the relations. Since k is prime to p, it follows that $\tilde{\alpha}$ is an automorphism of P and by definition $\tilde{\alpha}$ extends α.

The element z has order $p^{\max\{m,s\}}$. Since $m, s \geq 1$, we have then $m < m+s$ and $s < m+s$. It follows that the definition of $\tilde{\alpha}$ is independent of the choice of a representative of k modulo p^{m+s}. The map sending $\alpha \in \mathrm{Aut}(U)$ to $\tilde{\alpha} \in \mathrm{Aut}(P)$ is a then a homomorphism. If $\tilde{\alpha}$ is the identity on P then by definition $\tilde{\alpha}$ is the identity on U so that this homomorphism $\mathrm{Aut}(U) \to \mathrm{Aut}(P)$ is injective and the lemma is proved. □

Let $w \in Z(P)$ be defined by

$$w = \begin{cases} y_\ell^{p^m} & \text{if } s \leq m. \\ y_\ell^{p^s} & \text{if } m \leq s. \end{cases}$$

Let θ be the automorphism of U defined by $\theta(y_\ell) = y_\ell w$, that is

$$\theta(y_\ell) = \begin{cases} y_\ell^{1+p^m} & \text{if } s \leq m \\ y_\ell^{1+p^s} & \text{if } m \leq s \end{cases}$$

We denote also θ its extension to the whole group P given by Lemma 3.5.5. Remark then that θ is the identity on all generators except y_ℓ.

Lemma 3.5.6. *The intersection* $\mathrm{Aut}(U) \cap \mathrm{Aut}_{Z(P)}(P)$ *is generated by* $\langle\theta\rangle$ *and in particular is cyclic of order* $p^{\min\{m,s\}}$.

Proof. We first show that $\theta(w) = w$. If $s \leq m$, then $\theta(w) = w^{1+p^m} = ww^{p^m}$. But w has order p^s with $s \leq m$ so that $w^{p^m} = 1$ and hence $\theta(w) = w$. A similar argument shows that $\theta(w) = w$ also when $m \leq s$.

We have then that $\theta^a(y_\ell) = y_\ell w^a$. It follows that θ has the same order as w, hence θ has order p^s if $s \leq m$ and order p^m if $m \leq s$.

When $s \leq m$, we have $z = [x_\ell, y_\ell]$ so that $\theta(z) = [x_\ell, y_\ell w] = z$ since w is central. When $m \geq s$, we have $z = y^{p^m}$ and hence $\theta(z) = y^{p^m} w^{p^m} = z$ since $w^{p^m} = 1$. It follows that in both cases $\theta(z) = z$ so that $\theta \in \mathrm{Aut}(U) \cap \mathrm{Aut}_{Z(P)}(P)$.

It remains to show that θ generates $\mathrm{Aut}(U) \cap \mathrm{Aut}_{Z(P)}(P)$. If $\alpha \in \mathrm{Aut}(U) \cap \mathrm{Aut}_{Z(P)}(P)$ is given by $\alpha(y_\ell) = y_\ell^k$ then $z = \alpha(z) = z^k$. If $s \leq m$, this implies that $k = 1 + ap^m$ for some a. It follows that $\alpha(y_\ell) = y_\ell w^a$ and hence $\alpha = \theta^a$. A similar argument shows that $\alpha \in \langle\theta\rangle$ also when $m \leq s$ and the lemma is proved. □

Since $Z(P)$ is characteristic, there is a well-defined map

$$\pi : \mathrm{Aut}_{Z(P)}(P) \to \mathrm{Aut}(P/Z(P)).$$

Furthermore, the image of $\theta \in \mathrm{Aut}_{Z(P)}(P)$ must preserve the non-degenerate alternating form b on $P/Z(P)$ induced by commutators and the linear form φ induced by p^m-th powers. We denote $Sp_\varphi(P/Z(P))$ the subgroup of $Sp(P/Z(P))$ consisting of all automorphisms of $P/Z(P)$ preserving b and φ, namely

$$Sp_\varphi(P/Z(P)) = \{\alpha \in \mathrm{Aut}(P/Z(P)) \,|\, b(\alpha v, \alpha w) = b(v, w) \text{ and } \varphi(\alpha v) = \varphi(v), \\ \forall v, w \in P/Z(P)\}$$

Lemma 3.5.7. *The image of* π *is contained in* $Sp_\varphi(P/Z(P))$.

Proof. If α is an automorphism of P fixing $Z(P)$ pointwise, then by definition $\pi(\alpha)(\overline{x}) = \overline{\alpha(x)}$ and thus

$$b(\overline{x}, \overline{y}) = [x, y] = \alpha([x, y]) = [\alpha x, \alpha y] = b(\overline{\alpha(x)}, \overline{\alpha(y)}) = b(\pi(\alpha)(\overline{x}), \pi(\alpha)(\overline{y})).$$

Therefore $\pi(\alpha)$ preserves the non-degenerate alternating form b induced by the commutators. We have furthermore $\alpha(x^{p^m}) = x^{p^m}$, since $x^{p^m} \in Z(P)$ for all $x \in P$. Therefore $\varphi(\pi(\alpha)(v)) = \varphi(v)$ for all $v \in P/Z(P)$ and the lemma is proved. □

Lemma 3.5.8. *The kernel of* π *is equal to the group* $\mathrm{Int}(P)$ *of inner automorphisms of* P.

Proof. We set $r = 0$ if $s \leq m$ and $r = s - m$ if $m \leq s$, so that in both cases $|Z(P)|$ has order p^{m+r}. It follows from Lemma 3.2.1 that

$$\ker\psi \cong \mathrm{Hom}(P/Z(P), Z(P)) = \mathrm{Hom}((C_{p^m})^{2\ell}, C_{p^{m+r}}) \cong (C_{p^m})^{2\ell}.$$

Since also $\mathrm{Int}(P) \cong P/Z(P) \cong (C_{p^m})^{2\ell}$, it remains to show that $\mathrm{Int}(P)$ is contained in $\ker\pi$. This follows as usual from the fact that the commutators are central in P and the lemma is proved. □

Proposition 3.5.9. *Let $P = X_3(p^m)^{*(\ell-1)} * M(m,s)$ with $\ell \geq 1$ and $s \geq 1$. Then $\mathrm{Aut}(P)$ is generated by $\mathrm{Aut}_{Z(P)}(P)$ and a subgroup $H \cong \mathrm{Aut}(C_{p^{m+s}})$. Furthermore, $H \cap \mathrm{Aut}_{Z(P)}(P)$ is cyclic of order $p^{\min\{m,s\}}$ and there is an exact sequence*

$$1 \to \mathrm{Int}(P) \to \mathrm{Aut}_{Z(P)}(P) \to S \to 1$$

where S is isomorphic to the subgroup of $Sp_{2\ell}(\mathbb{Z}/p^m\mathbb{Z})$ consisting of matrices s such that $s_{2\ell,j} = 0$ for $j = 1, \ldots, 2\ell - 1$ and

$$s_{2\ell,2\ell} \equiv \begin{cases} 1 \mod p^s & \text{if } s \leq m. \\ 1 \mod p^m & \text{if } m \leq s. \end{cases}$$

Proof. We show first that the group $Sp_\varphi(P/Z(P))$ is isomorphic to S. In view of the preceding lemmas, it will then only remain to show that the map $\pi : \mathrm{Aut}_{Z(P)}(P) \to \mathrm{Aut}(Z(P))$ is surjective on $Sp_\varphi(P/Z(P))$.

To begin, we reorder the elements $x_1, y_1, \ldots, x_\ell, y_\ell$. For $j = 1, \ldots, \ell$ we let $w_j = x_j$ and $w_{j+\ell} = y_j$. We have this way

$$[w_j, w_k] = z^{p^r}, \text{ if } |j-k| = \ell,$$
$$[w_j, w_k] = 1, \text{ else.}$$

Furthermore, w_j has order p^m for $1 \leq j \leq 2\ell - 1$ and

$$w_{2\ell}^{p^m} = \begin{cases} z^{p^{m-s}} & \text{if } s \leq m. \\ z & \text{if } m \leq s. \end{cases}$$

Let $\mathcal{B} = \{\overline{w}_1, \ldots, \overline{w}_{2\ell}\}$ be the basis of $P/Z(P)$ where $\overline{w}_i$ is the class of w_i in $P/Z(P)$. Relatively to this basis, the alternating form b is represented by the matrix

$$\begin{pmatrix} 0 & I_\ell \\ I_\ell & 0 \end{pmatrix}.$$

Relatively to this basis the group $Sp_\varphi(P/Z(P))$ is isomorphic to a subgroup of the symplectic group $Sp_{2\ell}(\mathbb{Z}/p^m\mathbb{Z})$. Let s be the matrix of $\alpha \in Sp_\varphi(P/Z(P))$, that is

$$\alpha(\overline{w}_i) = \sum_{k=1}^{2\ell} s_{k,j} \overline{w}_k.$$

Since α stabilizes the kernel of the linear form φ, we have that $s_{2\ell,j} = 0$ for all $j = 1, \ldots, 2\ell - 1$. Furthermore, $\alpha(\overline{w}_{2\ell}) = \lambda \overline{w}_{2\ell} + v$ with λ invertible in $\mathbb{Z}/p^m\mathbb{Z}$ and $v \in \ker \varphi$.

Suppose first $s \leq m$. In this situation, we have furthermore $y^{p^m} = z^{p^{m-s}}$, so that $\varphi(\overline{w}_{2\ell}) = p^{m-s}$. It follows that

$$p^{m-s} = \varphi(\overline{w}_{2\ell}) = \varphi(\alpha(\overline{w}_{2\ell})) = \lambda p^{m-s}$$

Therefore, $\lambda \equiv 1 \mod p^s$.

Suppose now $m \leq s$. In this situation, we have $y^{p^m} = z$ so that $\varphi(\overline{w}_{2\ell}) = 1$. We must have then $\lambda \equiv 1 \mod p^m$.

It remains now to show that π is surjective on $Sp_{\varphi}(P/Z(P))$. We will show that any automorphism of $P/Z(P)$ preserving b and φ is induced by an automorphism of P. So let α be an automorphism of $P/Z(P)$ such that $\alpha(b(v,w)) = b(\alpha v, \alpha w)$ and $\varphi(\alpha(v)) = \varphi(v)$ for all $v, w \in P/Z(P)$. For any $x \in P$ we denote $\overline{x}$ its class in $P/Z(P)$. We have then

$$\alpha(\overline{w}_i) = \overline{w}_1^{s_{1,i}} \cdots \overline{w}_{2\ell}^{s_{2\ell,i}}$$

We define now $\tilde{\alpha} : P \to P$ to be the map with the following values on the generators of P

$$\begin{aligned} \tilde{\alpha}(z) &= z, \\ \tilde{\alpha}(w_i) &= w_1^{s_{1,i}} \cdots w_{2\ell}^{s_{2\ell,i}}. \end{aligned}$$

The relations of the form $[w_i, w_{i+\ell}] = z^{p^r}$ are preserved because α preserves b. For $1 \leq j \leq 2\ell - 1$, the element $\alpha(w_i)$ has order p^m because α is invertible. Since α preserves φ we also have that the relation

$$w_{2\ell}^{p^m} = \begin{cases} z^{p^{m-s}} & \text{if } s \leq m. \\ z & \text{if } m \leq s. \end{cases}$$

is preserved. Therefore $\tilde{\alpha}$ is a well-defined automorphism of P and it is clear that $\tilde{\alpha}$ induces α on $P/Z(P)$. It follows that π is surjective on the group $Sp_{\varphi}(P/Z(P))$ and the lemma is proved. $\square$

Automorphisms of $X_{2(\ell-1)+1}(p^m) * M(m,s) * C_{p^{m+r}}$

Let $P = X_3(p^m)^{*(\ell-1)} * M(m,s) * C_{p^{m+r}}$ with $\ell \geq 1$ and $1 \leq r < s < m + r$. Let z be a generator of $Z(P)$, the group P is generated by z and elements $x_1, y_1, \ldots, x_\ell, y_\ell$ such that all except y_ℓ have order p^m and satisfy

$$\begin{aligned} [x_i, y_i] &= z^{p^r}, \\ [x_i, x_j] = [x_i, y_j] &= [y_i, y_j] = 1, \\ y_\ell^{p^m} &= z^{p^{m+r-s}}. \end{aligned}$$

Let U be the subgroup generated by y_ℓ. This is a cyclic subgroup of P of order p^{m+s} containing P'.

Lemma 3.5.10. *There is an injective homomorphism*

$$\mathrm{Aut}(U) \hookrightarrow \mathrm{Aut}(P)$$

Proof. An automorphism $\alpha \in \mathrm{Aut}(U)$ sends y_ℓ to y_ℓ^k for some k prime to p uniquely defined modulo p^{m+s}. We extend α to the whole group P by letting

$$\begin{aligned} \tilde{\alpha}(x_i) &= x_i, \\ \tilde{\alpha}(y_i) &= y_i^k, \\ \tilde{\alpha}(z) &= z^k. \end{aligned}$$

As defined, $\tilde{\alpha}$ preserves all the relations. Since k is prime to p, it follows that $\tilde{\alpha}$ is an automorphism of P and by definition $\tilde{\alpha}$ extends α.

The element z has order p^{m+r} and $m+r < m+s$ since $r < s$. It follows that the definition of $\tilde{\alpha}$ is independent of the choice of a representative of k modulo p^{m+s}. The map sending $\alpha \in \mathrm{Aut}(U)$ to $\tilde{\alpha} \in \mathrm{Aut}(P)$ is a then a homomorphism. If $\tilde{\alpha}$ is the identity on P then by definition α is the identity on U so that this homomorphism $\mathrm{Aut}(U) \to \mathrm{Aut}(P)$ is injective and the lemma is proved. □

We let $w = y_\ell^{p^{m+r}}$ and let θ be the automorphism of U defined by $\theta(y_\ell) = y_\ell^{1+p^{m+r}} = y_\ell w$. We denote also θ its extension to the whole group P given by the previous lemma. Remark then that θ is the identity on all generators except y_ℓ. Furthermore, $\theta(w) = w^{1+p^{m+r}} = w$ since w has order p^{s-r} and $m + r > s > s - r$. It follows that $\theta^a(y_\ell) = y_\ell w^a$ and in particular θ has order p^{s-r}.

Lemma 3.5.11. *The intersection* $\mathrm{Aut}(U) \cap \mathrm{Aut}_{Z(P)}(P)$ *is cyclic of order* p^{s-r} *and generated by the automorphism* θ.

Proof. We have $\theta(z) = z^{1+p^{m+r}} = z$ since z has order p^{m+r}. We have then $\theta \in \mathrm{Aut}(U) \cap \mathrm{Aut}_{Z(P)}(P)$ and it remains to show that θ generates $\mathrm{Aut}(U) \cap \mathrm{Aut}_{Z(P)}(P)$.

An automorphism $\alpha \in \mathrm{Aut}(U) \cap \mathrm{Aut}_{Z(P)}(P)$ is given by $\alpha(y_\ell) = y_\ell^k$ for some k prime to p. Since $\alpha(z) = z$ and z has order p^{m+r}, we must have $k \equiv 1 \mod p^{m+r}$. Therefore, $\alpha(y_\ell) = y_\ell y^{ap^{m+r}} = y_\ell w^a$ for some a, so that $\alpha = \theta^a$ and the lemma is proved. □

Since $Z(P)$ is characteristic, there is a canonical homomorphism

$$\pi : \mathrm{Aut}_{Z(P)}(P) \to \mathrm{Aut}(P/Z(P)).$$

Furthermore, the image of $\theta \in \mathrm{Aut}_{Z(P)}(P)$ must preserve the non-degenerate alternating form b on $P/Z(P)$ induced by commutators and the linear form φ induced by p^m-th powers. As before, we denote $Sp_\varphi(P/Z(P))$ the subgroup of $Sp(P/Z(P))$ consisting of all automorphisms of $P/Z(P)$ preserving b and φ.

Lemma 3.5.12. *The image of* π *is contained in* $Sp_\varphi(P/Z(P))$.

Proof. If α is an automorphism of P fixing $Z(P)$ pointwise, then by definition $\pi(\alpha)(\overline{x}) = \overline{\alpha(x)}$ and thus

$$b(\overline{x}, \overline{y}) = [x, y] = \alpha([x, y]) = [\alpha x, \alpha y] = b(\overline{\alpha(x)}, \overline{\alpha(y)}) = b(\pi(\alpha)(\overline{x}), \pi(\alpha)(\overline{y})).$$

Therefore $\pi(\alpha)$ preserves the non-degenerate alternating form b induced by the commutators. We have furthermore $\alpha(x^{p^m}) = x^{p^m}$, since $x^{p^m} \in Z(P)$ for all $x \in P$. Therefore $\varphi(\pi(\alpha)(v)) = \varphi(v)$ for all $v \in P/Z(P)$ and the lemma is proved. □

Lemma 3.5.13. *The kernel of* π *is equal to the group* $\mathrm{Int}(P)$ *of inner automorphisms of* P.

Proof. The kernel of π consists of all automorphisms of P fixing $Z(P)$ and $P/Z(P)$ pointwise. It follows from Lemma 3.2.1 that

$$\ker \pi \cong \mathrm{Hom}(P/Z(P), Z(P)) \cong \mathrm{Hom}((C_{p^m})^{2\ell}, C_{p^{m+r}}) \cong (C_{p^m})^{2\ell}.$$

The two groups $\mathrm{Int}(P)$ and $\ker \pi$ have then the same order since $\mathrm{Int}(P) \cong P/Z(P) \cong (C_{p^m})^{2\ell}$. Furthermore, $\mathrm{Int}(P)$ is contained in $\ker \pi$ since P' is central in P and the lemma is proved. □

Proposition 3.5.14. *Let $P = X_3(p^m)^{*(\ell-1)} * M(m,s) * C_{p^{m+r}}$ with $\ell \geq 1$ and $1 \leq r < s < m+r$. Then $\mathrm{Aut}(P)$ is generated by $\mathrm{Aut}_{Z(P)}(P)$ and a subgroup $H \cong \mathrm{Aut}(C_{p^{m+s}})$. Furthermore, $H \cap \mathrm{Aut}_{Z(P)}(P)$ is cyclic of order p^{s-r} and there is an exact sequence*

$$1 \to \mathrm{Int}(P) \to \mathrm{Aut}_{Z(P)}(P) \to Sp_\varphi(P/Z(P)) \to 1$$

Proof. We show first that π is surjective on $Sp_\varphi(P/Z(P))$. To begin, we reorder the elements $x_1, y_1, \ldots, x_\ell, y_\ell$. For $j = 1, \ldots, \ell$ we let $w_j = x_j$ and $w_{j+\ell} = y_j$. We have this way

$$[w_j, w_k] = \begin{cases} z^{p^r} & \text{if } |j-k| = \ell, \\ 1 & \text{else.} \end{cases}$$

We will show that any automorphism of $P/Z(P)$ preserving b and φ is induced by an automorphism of P. So let α be an automorphism of $Z(P)$ such that $\alpha(b(v,w)) = b(\alpha v, \alpha w)$ and $\varphi(\alpha(v)) = \varphi(v)$ for all $v, w \in P/Z(P)$. For any $x \in P$ we denote $\overline{x}$ its class in $P/Z(P)$. We have then

$$\alpha(\overline{w}_i) = \overline{w}_1^{s_{1,i}} \cdots \overline{w}_{2\ell}^{s_{2\ell,i}}$$

We define now $\tilde{\alpha} : P \to P$ to be the map with the following values on the generators of P

$$\tilde{\alpha}(z) = z,$$
$$\tilde{\alpha}(w_i) = w_1^{s_{1,i}} \cdots w_{2\ell}^{s_{2\ell,i}}.$$

Since α preserves the alternating form b and the linear form φ all relations are preserved, so that $\tilde{\alpha}$ is an automorphism of P. By definition, $\tilde{\alpha}$ induces α on $P/Z(P)$. It follows that π is surjective on the group $Sp_\varphi(P/Z(P))$ and we describe now this group more precisely

Let $\mathcal{B} = \{\overline{w}_1, \ldots, \overline{w}_{2\ell}\}$ be the basis of $P/Z(P)$ where $\overline{w}_i$ is the class of w_i in $P/Z(P)$. Relatively to this basis, the alternating form b is represented by the matrix

$$\begin{pmatrix} 0 & I_\ell \\ I_\ell & 0 \end{pmatrix}.$$

Relatively to this basis the group $Sp_\varphi(P/Z(P))$ is isomorphic to a subgroup of the symplectic group $Sp_{2\ell}(p^m)$. Let s be the matrix of $\alpha \in S$, that is

$$\alpha(\overline{w}_i) = \sum_{k=1}^{2\ell} s_{k,j} \overline{w}_k.$$

Since α stabilizes the kernel of the linear form φ, we have that $s_{2\ell,j} = 0$ for all $j = 1, \dots, 2\ell - 1$. Furthermore, $\alpha(\overline{w}_{2\ell}) = \lambda \overline{w}_{2\ell} + v$ with λ invertible in $\mathbb{Z}/p^m\mathbb{Z}$ and $v \in \ker \varphi$. We have furthermore $y^{p^m} = z^{p^{m+r-s}}$ so that

$$\varphi(\overline{w}_{2\ell}) \equiv p^{m+r-s} \mod p^m.$$

Since α preserves φ we also have

$$\varphi(\overline{w}_{2\ell}) = \varphi(\alpha(\overline{w}_{2\ell})) = \lambda\varphi(\overline{w}_{2\ell})$$

It follows that $\lambda \equiv 1 \mod p^{s-r}$ and the proposition is proved. □

Appendix A

Alternating forms

Definitions and first properties

Let R be a commutative ring with unit and let M be a finitely generated R-module.

Definition A.0.1. An alternating form on M is an R-bilinear form

$$b : M \times M \to R,$$

such that $b(x, x) = 0$, for all $x \in M$. We will call the pair (M, b) an alternating module. If furthermore $M = L$ is free over R, then we call (L, b) an alternating space.

Remark A.0.2. The condition $b(x, x) = 0$ implies that $b(y, x) = -b(x, y)$. The converse is also true provided that the characteristic of R odd.

Definition A.0.3. The orthogonal sum of two alternating modules (M, b) and (M', b') is the alternating module $(M \oplus M', b \oplus b')$ with

$$(b \oplus b')(x + x', y + y') = b(x, y) + b'(x', y'), \text{ for all } x, y \in M \text{ and } x', y' \in M'.$$

We fix now an alternating form b on M.

Definition A.0.4. Let N be a submodule of M, the orthogonal complement of N in M (with respect to b) is the submodule $N^\perp$ of M defined by

$$N^\perp = \{x \in M \,|\, b(x, y) = 0 \text{ for all } y \in N\}.$$

Definition A.0.5. The alternating form b induces an R-linear map $\hat{b} : M \to M^* = \hom(M, R)$ defined by $\hat{b}(x)(y) = b(x, y)$. The map $\hat{b}$ is called the adjoint map to b.

It is easy to see that $\ker \hat{b} = M^\perp$ so that in particular $M^\perp = 0$ if and only if $\hat{b}$ is injective. But it is important to note that it does not necessarily imply that $\hat{b}$ is an isomorphism. As a counterexample, one can consider the case $R = \mathbb{Z}$, $M = \mathbb{Z}^2$ and b given by $b(x, y) = 2x_1y_2 - 2x_2y_1$ for $x = (x_1, x_2), y = (y_1, y_2) \in \mathbb{Z}^2$.

Lemma A.0.6. *If either R is a field or R is finite and M is free over R, then $M^\perp = 0$ if and only if $\hat{b}$ is an isomorphism.*

Proof. If R is a field, then M and M^* are vector spaces over R of the same dimension. In particular, any injective map $M \to M^*$ is also surjective. The same is true if R is finite and M is free over R, say of rank r, since in this situation $M^* = \mathrm{Hom}(M, R) \cong \mathrm{Hom}(R^r, R) \cong R^r$. Hence $\hat{b}$ can be seen as a map $R^r \to R^r$ and since R is finite $\hat{b}$ is injective if and only if $\hat{b}$ is surjective. This shows that the condition $M^\perp = 0$ implies that $\hat{b}$ is an isomorphism. The converse is trivial. □

Definition A.0.7. The alternating form b is said to be non-degenerate if $M^\perp = 0$.

Definition A.0.8. The alternating form b is said to be regular if $\hat{b}$ is an isomorphism.

In the setting of vector spaces or free module over finite rings, these two definitions coincide and regular and non-degenerate are often considered to be synonyms. Since we work here in a more general setting, we will keep the distinction. It is of particular importance in the following crucial lemma. Recall that if N is a submodule, the restriction of b to N is the alternating form $b_N : N \times N \to R$ given by $b_N(x, y) = b(x, y)$ for all $x, y \in N$.

Proposition A.0.9. *Let b be an alternating form on the R-module M and let N be a submodule of M such that the restriction b_N of b on N is regular. Then $M = N \oplus N^\perp$.*

Proof. By definition, $N \cap N^\perp = \ker\left(\widehat{b_N} : N \to \mathrm{Hom}(N, R)\right)$, hence $N \cap N^\perp = 0$, since b_N is non-degenerate.

Let $x \in M$, then $\hat{b}(x) \in \mathrm{Hom}(M, R)$ and we can consider its restriction to N, namely $\hat{b}(x)_N \in \mathrm{Hom}(N, R)$. Since b_N is regular, there exists $y \in N$ such that $\hat{b}(x)_N = \widehat{b_N}(y)$ and now $x = y + (x - y) \in N + N^\perp$.

This shows that $M = N \oplus N^\perp$ and it is clear that the sum is orthogonal. □

Alternating forms on vector spaces

Let $R = \mathbb{F}$ be a field and let $M = V$ be a vector space over $\mathbb{F}$.

Proposition A.0.10. *If $b : V \times V \to \mathbb{F}$ is a non-degenerate alternating form on V, then $\dim V$ is even, say $\dim V = 2n$, and there exists a basis $e_1, f_1, \ldots, e_n, f_n$ of V such that*

$$b(e_i, f_i) = 1, \text{ for all } i = 1, \ldots, n, \tag{A.1}$$

$$b(e_i, e_j) = b(e_i, f_j) = b(f_i, f_j) = 0, \text{ for all } 1 \leq i \neq j \leq n. \tag{A.2}$$

Proof. Since b is non-degenerate, there exist $x, y \in V$ such that $b(x,y) \neq 0$. By multipliying x or y by a scalar, one can suppose that $b(x,y) = 1$. Let W be the subspace of V generated by x and y. It is easy to see that the restriction b_W is non-degenerate on W, so that $V = W \oplus W^{\perp}$. Of course this sum is orthogonal and the proposition follows by a recursive argument. □

Definition A.0.11. If b is a non-degenerate alternating form V, then a basis of V satisfying conditions (A.1) and (A.2) is called a symplectic basis.

If $\varphi : V \to \mathbb{F}$ is a non-zero linear form on V, then the kernel of φ has codimension 1 in V. The following proposition shows that the symplectic basis can be chosen such that all but one of the elements of the basis are in $\ker \varphi$.

Proposition A.0.12. *Let b be a non-degenerate alternating form on V and let $\varphi : V \to \mathbb{F}$ be a linear map on V. There exists a symplectic basis $e_1, f_1, \ldots, e_n, f_n$ on V such that $\varphi(e_i) = \varphi(f_i) = \varphi(e_n) = 0$ for all $i = 1, \ldots, n-1$ and $\varphi(f_n) = 1$.*

Proof. Since $\hat{b}$ is linear, there exist e in V such that $\hat{b}(e) = \varphi$. In particular, $\varphi(e) = b(e,e) = 0$ and if we choose $f \in V$ such that $b(e,f) = 1$, then $\varphi(f) = 1$. Let W be the subspace of V generated by e and f. The restriction b_W is non-degenerate, so that $V = W \oplus W^{\perp}$. For $u \in W^{\perp}$, we have $\varphi(w) = b(e,w) = 0$, so that $W^{\perp}$ is contained in $\ker \varphi$. Now, the restriction $b_{W^{\perp}}$ is also non-degenerate so that we can choose a symplectic basis $e_1, f_1, \ldots, e_{n-1}, f_{n-1}$ on $W^{\perp}$ and if we let $e_n = e$ and $f_n = f$ we obtain the desired basis. □

Alternating forms on $\mathbb{Z}/p^m\mathbb{Z}$-modules

Definition A.0.13. Let L be a free R-module and let b be an alternating form on L. A symplectic basis on L is a basis $e_1, f_1, \ldots, e_n, f_n$ of L such that

$$b(e_i, f_i) = 1, \text{ for all } i = 1, \ldots, n,$$
$$b(e_i, e_j) = b(e_i, f_j) = b(f_i, f_j) = 0, \text{ for all } 1 \leq i \neq j \leq n.$$

When $R = \mathbb{Z}/p^m\mathbb{Z}$ and $M = L$ is free over R, the situation is very similar to the situation of alternating spaces over fields, as the two next results show.

Proposition A.0.14. *If (L, b) is a regular alternating space over $R = \mathbb{Z}/p^m\mathbb{Z}$, then the rank of L is even and there exists a symplectic basis on L.*

Proof. Since b is regular, L has rank at least 2 and let $x_1, \ldots, x_r$ be a basis of L. We claim that there exists $1 < j \leq r$ such that $b(x_1, x_j)$ has order p^m. Indeed, if $b(x_1, x_j)$ has order strictly less that p^m for all j, then there exists $a < m$ such that $p^a b(x_1, x_j) = 0$. But then, one would have $b(p^a x_1, x_j) = 0$ for all j, so that $p^a x_1 \in L^{\perp}$. Since b is regular, this would imply $p^a x_1 = 0$ for an $a < m$ which is a contradiction since x_1 is a basis element. Let $e_1 = x_1$ and $f_1 = x_j$ where j is such that $b(x_1, x_j)$ has order p^m. By rescaling x_1, we can assume that $b(e_1, f_1) = 1$. Let N be the submodule of L generated by e_1 and f_1. It is easy to see that N is free and that the restriction b_N is regular. Hence $M = N \oplus N^{\perp}$. Remark that $N^{\perp}$ is a free $\mathbb{Z}/p^m\mathbb{Z}$-module, since both M and N are homocyclic abelian groups of type p^m. A more elaborate argument would be to say that both M and N are free over $\mathbb{Z}/p^m\mathbb{Z}$ and that Krull-Schmidt holds for $\mathbb{Z}/p^m\mathbb{Z}$. The proof follows now by an induction argument. $\square$

Lemma A.0.15. *Let (L, b) be a regular alternating space over $R = \mathbb{Z}/p^m\mathbb{Z}$ and let φ be a linear form on L. There exists a symplectic basis $e_1, f_1, \ldots, e_n, f_n$ on L such that $\varphi(f_n) = p^a$ for some $0 \leq a \leq m-1$ and φ is zero on all other elements of the basis.*

Proof. Since b is regular, there exists $x \in L$ such that $\varphi = \hat{b}(x)$. Let $x_1, \ldots, x_s$ be a basis of L. Then $x = \sum_{i=1}^{s} \overline{n_i} x_i$, where we use $\bar{\cdot}$ to denote the class of an integer modulo p^m. Now, we can rewrite $x = p^a \sum_{i=1}^{s} \overline{m_i} x_i$ with $a \geq 0$ and m_j is prime to p for some j. Without loss of generality, we may suppose that m_1 is prime to p, so that in particular $\overline{m_1}$ is invertible in R. Let $x_1' = \sum_{i=1}^{s} \overline{m_i} x_i$, so that $x = p^a x_1'$. We claim that $x_1', x_2, \ldots, x_s$ is a basis of L. Since $x_1 = \overline{m_1}^{-1}(x_1' - \sum_{j=2}^{s} \overline{m_j} x_j)$, it clearly generates L. Now, if $r_1 x_1' + \sum_{j=2}^{s} r_j x_j = 0$ then

$$r_1 \overline{m_1} x_1 + \sum_{j=2}^{s} (r_1 \overline{m_j} + r_j) = 0$$

But then $r_1 = 0$ since $\overline{m_1}$ is invertible and it follows then that $r_j = 0$ for all $j = 2, \ldots, s$. Hence our claim is proved and we have shown that the basis of L can be chosen such that $\varphi = \hat{b}(p^a x_1)$. Let $e_n = x_1$. Following the proof of proposition A.0.14, we can find an element f_n and elements $e_1, f_1, \ldots e_{n-1}, f_{n-1}$ such that $e_1, f_1, \ldots, e_n, f_n$ is a symplectic basis. In particular, $\varphi(f_n) = b(p^s e_n, f_n) = p^a b(e_n, f_n) = p^a$. $\square$

Proposition A.0.16. *For $m \geq 1$, let $R = \mathbb{Z}/p^m\mathbb{Z}$ and let b be a regular alternating form on the R-module M. Then M can be decomposed as an orthogonal sum $M = (M_1, b_1) \oplus \cdots \oplus (M_s, b_s)$, where (M_i, b_i) is a regular alternating space over $\mathbb{Z}/p^{m_i}\mathbb{Z}$ with $m \geq m_1 > \cdots > m_s$ and such that $b_{M_i} = \tau_i b_i$ where $\tau_i : \mathbb{Z}/p^{m_i}\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ is the canonical injection sending the class of 1 modulo m_i to the class of p^{m-m_i} modulo m.*

Proof. Since b is regular, M has p-rank at least 2 and let $x, y \in M$ be such that $b(x, y)$ has maximal order, say p^{m_1}. By maximality of $b(x, y)$, we have for any $u, v \in M$ that $0 = p^{m_1} b(u, v) = b(p^{m_1} u, v)$ and since b is regular this implies that any $u \in M$ has order at most p^{m_1}. We claim that both x and y have order exactly p^{m_1}. Let p^a be the order of x. We already know that $a \leq m_1$. Now by maximality of the order of $b(x, y)$ we have $0 = p^{m_1} b(x, u) = b(p^{m_1} x, u)$ hence $p^{m_1} x \in M^{\perp}$. Since b is regular, this implies that $p^{m_1} x = 0$, hence $a \geq m_1$. The same argument shows that y has order p^{m_1}.

Let N be the submodule of M generated by x and y. Since x and y both have order p^{m_1} it follows that N is a free module of rank 2 over $\mathbb{Z}/p^{m_1}\mathbb{Z}$ and we claim that the restriction b_N is regular. Suppose $ax + a'y \in N$ is orthogonal to every other element of N. In particular $0 = b(ax + a'y, y) = a \cdot b(x, y)$ hence p^{m_1} divides a, but then $ax = 0$. A similar argument shows that $a'y = 0$ and therefore b_N is regular. The submodule N is then a regular alternating space over $\mathbb{Z}/p^{m_1}\mathbb{Z}$.

It follows in particular that $M = N \oplus N^{\perp}$ and an induction argument shows that $N^{\perp}$ decomposes as an orthogonal sum $N^{\perp} = N_1 \oplus \ldots \oplus N_t$ where (N_i, b_{N_i}) is a regular alternating space over $\mathbb{Z}/p^{n_i}\mathbb{Z}$ with $n_1 > n_2 > \ldots > n_t$. By maximality of the order of $b(x, y)$ we have $m_1 \geq n_1$. If $m_1 = n_1$ we set $M_1 = N \oplus N_1$ and $M_i = N_i$ for $i \geq 2$. If $m_1 > n_1$ we set $M_1 = N_1$ and $M_i = N_{i-1}$ for $i \geq 2$. This gives the desired decomposition of M. □

Quadratic forms in characteristic 2

We will recall here only the results for quadratic forms on vector spaces over the field $\mathbb{F}_2$. The reader will find more details for arbitrary fields in [28].

Definition A.0.17. A quadratic form on a K-vector space V is a map q from V to K such that $q(\lambda v) = \lambda^2 q(v)$ and $b(v, w) := q(u + v) - q(u) - q(v)$ is a bilinear form. The bilinear form b is called the polar form of q.

Definition A.0.18. The quadratic form q is non-degenerate if the condition $b(v, w) = q(v) = 0$ for all $w \in V$, implies $v = 0$.

Remark A.0.19. The quadratic form may be non-degenerate without its polar form being non-degenerate.

Proposition A.0.20. *Let q be a non-degenerate quadratic form on V with polar form b. If the dimension of V is odd, say $2n + 1$, then V has a basis $e_1, f_1, \ldots, e_n, f_n, c$ such that*

$$\begin{gathered} b(e_i, f_i) = 1 \\ b(e_i, e_j) = b(e_i, f_j) = b(f_i, f_j) = 0 \text{ for } i \neq j \\ b(e_i, c) = b(f_i, c) = 0 \\ q(e_i) = q(f_i) = 0 \\ q(c) = 1 \end{gathered}$$

If V has dimension even, say $2n$, then V has a basis $e_1, f_1, \ldots, e_n, f_n$ such that

$$\begin{gathered} b(e_i, f_i) = 1 \\ b(e_i, e_j) = b(e_i, f_j) = b(f_i, f_j) = 0 \text{ for } i \neq j \end{gathered}$$

and either

$$q(e_i) = q(f_i) = 0 \text{ for all } i = 1, \ldots, n$$

or

$$\begin{gathered} q(e_i) = q(f_i) = 0 \text{ for all } i = 1, \ldots, n-1 \\ q(e_n) = q(f_n) = 1 \end{gathered}$$

Remark A.0.21. In all cases, the basis elements e_i, f_i form a symplectic basis (relatively to b) of the subspace they generate.

Appendix B

A note on the orthogonal group $O(2\ell+1,2)$

The purpose of this appendix is to show a small result on the orthogonal group $O(2\ell+1,2)$ that was needed in chapter 3. It is a well-known fact that the orthogonal group $O(2\ell+1,2)$ is isomorphic to the symplectic group $Sp(2\ell,2)$ and let us recall briefly where this isomorphism comes from.

Let (V,q) be a non-degenerate quadratic space of odd dimension $2\ell+1$ over the field $\mathbb{F}_2$. Let b be the polar form of q. Since V has odd dimension and q is non-degenerate, we have that $V^\perp$ has dimension 1 and does not contain any non-singular vector. This means that if w is the basis element of $V^\perp$ then $q(w)=1$. The vector space V has a basis $\mathcal{B}=\{e_1,\dots,e_{2\ell},w\}$ such that $q(e_i)=0$ for all $i=1,\dots,2\ell$ and

$$b(e_i,e_j)=\begin{cases}1 & \text{if } |i-j|=\ell.\\ 0 & \text{else.}\end{cases}$$

The alternating form b induces naturally a non-degenerate alternating form $\overline{b}$ on $\overline{V}=V/V^\perp$. If α is in the orthogonal group $O(V,q)=O(2\ell+1,q)$, then α induces a linear transformation $\overline{\alpha}$ on $\overline{V}$. Since α preserves the quadratic form and hence preserves b, we have that $\overline{\alpha}$ preserves $\overline{b}$ so that $\overline{\alpha}$ is in the symplectic group $Sp(\overline{V},\overline{b})=Sp(2\ell,2)$. We have thus a homomorphism

$$g: O(V,q)\to Sp(\overline{V},b)$$

sending α to $\overline{\alpha}$. With respect to the above basis $\{\mathcal{B}\}$, the automorphism α is represented by a matrix

$$A=\left(\begin{array}{ccccc|c} & & & & & 0\\ & & A' & & & \vdots\\ & & & & & 0\\ \hline q_1 & q_2 & \cdots & q_{2\ell-1} & q_{2\ell} & 1\end{array}\right).$$

Furthermore, A' is the matrix of $\overline{\alpha}$ relatively to the basis $\overline{\mathcal{B}}=\{\overline{e}_i, i=1,\dots,2\ell\}$ of $\overline{V}$. In particular, $A'\in Sp(2\ell,2)$.

It turns out that the coefficients q_i in the matrix of α are uniquely determined by A'. Indeed, since α preserves the quadratic form q and w is orthogonal to e_i for all $i = 1, \ldots, 2\ell$, we have

$$0 = q(e_i) = q(\alpha(e_i)) = q(A'e_i + q_i w) = q(A'e_i) + q_i q(w) = q(A'e_i) + q_i.$$

It follows then that

$$q_i = q(A'e_i). \tag{B.1}$$

This shows then directly that the homomorphism $g : O(V,q) \to Sp(\overline{V}, \overline{b})$ is injective. This last condition gives also the way of proving surjectivity. Indeed, if $\overline{\alpha}$ is in $Sp(\overline{V}, \overline{b})$, then $\overline{\alpha}$ is represented by a matrix A' relatively to the basis $\overline{\mathcal{B}}$. Let α be the linear transformation of V defined by

$$\begin{aligned} \alpha(e_i) &= A'e_i + q(A'e_i)w. \\ \alpha(w) &= w. \end{aligned}$$

Since $\overline{\alpha}$ preserves $\overline{b}$ we have that α preserves b. Furthermore, it follows by definition that $q(\alpha(e_i)) = 0 = q(e_i)$ and hence α preserves q. This shows that α is in $O(V,q)$ and the surjectivity of the homomorphism $g : O(V,q) \to Sp(\overline{V}, \overline{b})$ is proved.

Results on the group $O(2\ell+1,2)$ are generally obtained by considering the symplectic group $Sp(2\ell,2)$ instead. What interests us here concerns precisely what is left behind with this identification, namely the coefficients $q_1, \ldots, q_{2\ell}$. The purpose of this appendix is to prove the following result.

Proposition B.0.22. *Let (V,q) be non-degenerate quadratic space of odd dimension $2\ell+1$ over the field $\mathbb{F}_2$. Let $\mathcal{B} = \{e_1, \ldots, e_{2\ell}, w\}$ be a basis of V such that $w \in V^{\perp}$, the elements $\{e_i, i = 1, \ldots, 2\ell\}$ form a symplectic basis of the vector space V' they generate and $q(e_i) = 0$ for all $i = 1, \ldots, 2\ell$. If $\alpha \in O(V,q)$ is represented by the matrix*

$$\left(\begin{array}{ccccc|c} & & & & & 0 \\ & & A' & & & \vdots \\ & & & & & 0 \\ \hline q_1 & q_2 & \cdots & q_{2\ell-1} & q_{2\ell} & 1 \end{array}\right)$$

then $\sum_{k=1}^{\ell} q_k q_{k+\ell} = 0$.

Before going on with the proof of this proposition, we recall a little bit of terminology and notation. We make first the convention that all vector spaces are over the field $\mathbb{F}_2$.

If (V,q) is a quadratic space over $\mathbb{F}_2$, we will say that $v \in V$ is singular if $v \neq 0$ and $q(v) = 0$ and we will say that v is non-singular if $q(v) = 1$. We will call a hyperbolic line a 2-dimensional vector space $H = \langle e, f \rangle$ with $q(e) = q(f) = 0$ and $b(e,f) = 1$. A quadratic space is said to have type I if it is an orthogonal sum of hyperbolic lines.

For a quadratic space (L,q) of type I, we denote by $n_1(L)$ the number of non-singular vectors in L. Similarly, $n_0(L)$ is the cardinal of the set $\{x \in L \mid q(x) = 0\}$. We must have of course $n_0(L) + n_1(L) = 2^{\dim L}$.

If H is a hyperbolic line, then it is easy to see that $n_0(H) = 3$ and $n_1(H) = 1$. We see that there are thus more singular vectors than non-singular ones. We can give exact values for orthogonal sums of hyperbolic lines. The next result can easily be proved by a induction argument.

Lemma B.0.23. *If the vector space L is an orthogonal sum of ℓ hyperbolic lines, then*

$$n_0(L) = 2^{\ell-1}(2^\ell + 1) \quad \text{and} \quad n_1(L) = 2^{\ell-1}(2^\ell - 1)$$

We are now in position to prove Proposition B.0.22. The idea is roughly to use two different methods to count the number of singular vectors u such that $q(A'u) = q(u)$.

Proof of Proposition B.0.22. Let $u = \sum_{i=1}^{2\ell} x_i e_i \in V'$, we have

$$q(u) = \sum_{i=1}^{2\ell} q(x_i e_i) + \sum_{j=1}^{\ell} b(x_j e_j, x_{j+\ell} e_{j+\ell}) = \sum_{j=1}^{\ell} x_j x_{j+\ell}.$$

Since A' preserves the restriction of b to V' we have

$$q(A'u) = q\left(\sum_{i=2}^{2\ell} x_i A' e_i\right) = \sum_{j=1}^{\ell} q(x_j A' e_j + x_{j+\ell} A' e_{j+\ell}) = \sum_{i=1}^{2\ell} x_i q_i + \sum_{j=1}^{\ell} x_j x_{j+\ell}.$$

It follows that

$$q(A'u) = q(u) \iff \sum_{i=1}^{2\ell} x_i q_i = 0. \tag{B.2}$$

Let $q_0 = \sum_{j=1}^{\ell} (q_{\ell+j} e_j + q_j e_{\ell+j}) \in V'$. For any $u = \sum_{i=1}^{2\ell} x_i e_i \in V'$, we have

$$b(q_0, u) = \sum_{i=1}^{2\ell} x_i q_i.$$

Let $f : V' \to \mathbb{F}_2$ be the linear map defined by $f(u) = b(q_0, u) = \sum_{i=1}^{2\ell} x_i q_i$. We can now rewrite the previous condition (B.2) as

$$q(A'u) = q(u) \iff u \in \ker f = \langle q_0 \rangle^\perp.$$

Note that we have furthermore

$$q(q_0) = \sum_{j=1}^{\ell} q_j q_{j+\ell},$$

so that we are trying to prove that $q(q_0) = 0$.

If $f = 0$, then $q(A'u) = q(u)$ for all $v \in V$. Therefore $q_i = q(A'e_i) = q(e_i) = 0$ and the result follows trivially. We assume from now on that the linear form f is non-zero.

Let $V_1 = \{u \in V' \mid q(u) = 1\}$ be the set of non-singular vectors of V' and let similarly $V_0 = \{u \in V' \mid q(u) = 0\}$ the set of singular vectors together with 0.

The vector space V' is then a disjoint union $V' = V_0 \coprod V_1$. The subset V_1 is a disjoint union $V_1 = U_1 \coprod K_1$ where

$$K_1 = V_1 \cap \ker f = \{u \in V' \mid q(u) = 1 \text{ and } q(A'u) = q(u)\}$$

and

$$U_1 = \{u \in V' \mid q(u) = 1 \text{ and } q(A'u) \neq q(u)\}\,.$$

We decompose similarly $V_0 = U_0 \coprod K_0$. The transformation A' stabilizes the subsets K_0 and K_1 and exchanges the subsets U_0 and U_1. This shows in particular that $|U_1| = |U_0|$. By definition of these subsets, we have $\ker f = K_0 \coprod K_1$ an in particular $K_0 \coprod K_1$ has cardinality $2^{2\ell-1}$. Therefore,

$$2^{2\ell} = |V'| = |U_0| + |K_0| + |K_1| + |U_1| = 2|U_0| + 2^{2\ell-1}.$$

Hence $|U_0| = |U_1| = 2^{2\ell-2}$. By the previous Lemma B.0.23, we have also that $|V_0| = 2^{\ell-1}(2^\ell + 1)$ and $|V_1| = 2^{\ell-1}(2^\ell - 1)$. All this shows that

$$|K_0| = 2^{\ell-1}(2^{\ell-1} + 1)$$

and

$$|K_1| = 2^{\ell-1}(2^{\ell-1} - 1). \tag{B.3}$$

On the other hand, V' is a quadratic space of type I so that $\ker f = \langle q_0\rangle^\perp = V'' \oplus \langle q_0\rangle$ and V'' is a non-degenerate quadratic space of type I and dimension $2(\ell-1)$. Let $u'' = v'' + \lambda q_0 \in \langle q_0\rangle^\perp$ with $v'' \in V''$ and $\lambda \in \mathbb{F}_2$. Since q_0 is orthogonal to V'', we have

$$q(u'') = q(v'' + \lambda q_0) = q(v'') + \lambda q(q_0).$$

If $q(q_0) = 1$, the singular vectors in $\ker f = \langle q_0\rangle^\perp$ are the singular vectors in V'' together with the vectors $v'' + q_0$ with $q(v'') = 1$. It follows that the number of singular vectors in $\ker f$ is equal to the cardinality of V'', i.e.

$$|K_0| = 2^{2(\ell-1)}.$$

This is a contradiction to the value found previously in (B.3) and thus $q(q_0) = 0$. Since $q(q_0) = \sum_{j=1}^{\ell} q_j q_{j+\ell}$ the proposition is proved. □

Remark B.0.24. In the previous proof, the case $q(q_0) = 0$ yields no contradiction. Indeed, in this situation the non-singular vectors in $\ker f = \langle q_0\rangle^\perp$ have the form $u'' + \lambda q_0$ with $q(u'') = 1$ and $\lambda \in \mathbb{F}_2$. It follows then that

$$|K_1| = 2 \cdot n_1(V'') = 2 \cdot 2^{\ell-2}(2^\ell - 1) = 2^{\ell-1}(2^{\ell-1} - 1),$$

which is the value found in (B.3).

Bibliography

[1] Michael Aschbacher. *Finite group theory. 2nd ed.* Cambridge Studies in Advanced Mathematics. 10. Cambridge: Cambridge University Press. xi, 304 p. , 2000.

[2] D.J. Benson. *Representations and cohomology. II: Cohomology of groups and modules.* Cambridge Studies in Advanced Mathematics, 31. New York etc.: Cambridge University Press. x, 278 p. , 1991.

[3] D.J. Benson and Jon F. Carlson. The cohomology of extraspecial groups. *Bull. Lond. Math. Soc.*, 24(3):209–235, 1992.

[4] T. R. Berger, L. G. Kovács, and M. F. Newman. Groups of prime power order with cyclic Frattini subgroup. *Nederl. Akad. Wetensch. Indag. Math.*, 42(1):13–18, 1980.

[5] J.N.S. Bidwell, M.J. Curran, and D.J. McCaughan. Automorphisms of direct products of finite groups. *Arch. Math.*, 86(6):481–489, 2006.

[6] Anders Björner. A general homotopy complementation formula. *Discrete Math.*, 193(1-3):85–91, 1998.

[7] Anders Björner, Michelle L. Wachs, and Volkmar Welker. Poset fiber theorems. *Trans. Am. Math. Soc.*, 357(5):1877–1899, 2005.

[8] Serge Bouc and Jacques Thévenaz. The poset of elementary abelian subgroups of rank at least 2. *Monographies de L'Enseignement Mathématique*, 40:41–45, 2008.

[9] J.M. Brady, R.A. Bryce, and J. Cossey. On certain abelian-by-nilpotent varieties. *Bull. Aust. Math. Soc.*, 1:403–416, 1969.

[10] Kenneth S. Brown. Euler characteristics of groups: The p-fractional part. *Invent. Math.*, 29:1–5, 1975.

[11] Kaustuv Mukul Das. The Quillen complex of groups of symplectic type: the characteristic 2 case. *J. Algebra*, 223(2):556–561, 2000.

[12] Francesco Fumagalli. On the homotopy type of the Quillen complex of finite soluble groups. *J. Algebra*, 283(2):639–654, 2005.

[13] GAP – Groups, Algorithms, and Programming, Version 4.4.10. 2007.

[14] Daniel Gorenstein. *Finite groups. 2nd ed.* New York: Chelsea Publishing Company. XVII, 519 p. , 1980.

[15] Robert L.jun. Griess. Automorphisms of extra special groups and nonvanishing degree 2 cohomology. *Pac. J. Math.*, 48:403–422, 1973.

[16] Geir T. Helleloid. Automorphism Groups of Finite p-Groups: Structure and Applications. arXiv:0711.2816v1 [math.GR], 2007.

[17] Charles Hobby. Abelian subgroups of p-groups. *Pacific J. Math.*, 12:1343–1345, 1962.

[18] Charles Kratzer and Jacques Thévenaz. Type d'homotopie des treillis et treillis des sous-groupes d'un groupe fini. (Homotopy type of lattices and lattices of subgroups of a finite groups). *Comment. Math. Helv.*, 60:85–106, 1985.

[19] Y.K. Leong. Odd order nilpotent groups of class two with cyclic centre. *J. Aust. Math. Soc.*, 17:142–153, 1974.

[20] Y.K. Leong. Finite 2-groups of class two with cyclic centre. *J. Aust. Math. Soc., Ser. A*, 27:125–140, 1978.

[21] M.F. Newman. On a class of nilpotent groups. *Proc. Lond. Math. Soc., III. Ser.*, 10:365–375, 1960.

[22] Jürgen Pulkus and Volkmar Welker. On the homotopy type of the p-subgroup complex for finite solvable groups. *J. Aust. Math. Soc., Ser. A*, 69(2):212–228, 2000.

[23] Daniel Quillen. Homotopy properties of the poset of nontrivial p-subgroups of a group. *Adv. in Math.*, 28(2):101–128, 1978.

[24] John Shareshian. Hypergraph matching complexes and Quillen complexes of symmetric groups. *J. Comb. Theory, Ser. A*, 106(2):299–314, 2004.

[25] Radu Stancu. Almost all generalized extraspecial p-groups are resistant. *J. Algebra*, 249(1):120–126, 2002.

[26] Michio Suzuki. *Group theory. I*, volume 247 of *Grundlehren der Mathematischen Wissenschaften [FundamentalPrinciples of Mathematical Sciences]*. Springer-Verlag, Berlin, 1982. Translated from the Japanese by the author.

[27] Michio Suzuki. *Group theory. II*, volume 248 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1986. Translated from the Japanese.

[28] Donald E. Taylor. *The geometry of the classical groups.* Sigma Series in Pure Mathematics. 9. Berlin: Heldermann Verlag. v, 229 p. , 1992.

[29] J. Thévenaz and P.J. Webb. Homotopy equivalence of posets with a group action. *J. Comb. Theory, Ser. A*, 56(2):173–181, 1991.

[30] Michelle L. Wachs. Poset topology: tools and applications. In *Geometric combinatorics*, volume 13 of *IAS/Park City Math. Ser.*, pages 497–615. Amer. Math. Soc., Providence, RI, 2007.

[31] P. J. Webb. Subgroup complexes. In *The Arcata Conference on Representations of Finite Groups (Arcata, Calif., 1986)*, volume 47 of *Proc. Sympos. Pure Math.*, pages 349–365. Amer. Math. Soc., Providence, RI, 1987.

[32] David L. Winter. The automorphism group of an extraspecial p-group. *Rocky Mt. J. Math.*, 2:159–168, 1972.

Curriculum vitae

David Bornand
EPFL-SB-IGAT-CTG
Bâtiment de chimie UNIL
CH-1015 Lausanne
david.bornand@epfl.ch

Né le 10 mai 1979 à Baden (AG) et originaire de Sainte-Croix (VD).

Formation

Depuis 2004	Préparation d'une thèse de doctorat à l'EPFL
2004	Diplôme de mathématicien à l'Université de Lausanne
1998-2003	Etude de mathématiques à l'Université de Lausanne
1994-1997	Maturité scientifique à Lausanne

Pré-publications

2009	*Counterexamples to a Fiber Theorem*, 5p., to appear in *Journal of Algebra*.

Enseignement

Depuis 2004	Assistant à l'Université de Lausanne, puis à l'EPFL